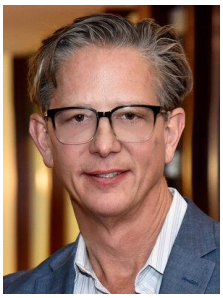
Navigating Data Privacy Assessments Amid New State Laws

By **Alan Friel and Sasha Kiosse** (May 22, 2023)



Alan Friel

Sasha Kiosse

This year, dozens of consumer privacy bills have been moving through state legislatures, and three became enacted.

So far in 2023, Iowa's Act Relating to Consumer Data Protection,[1] Indiana's Consumer Data Protection Act[2] and Tennessee's Information Protection Act[3] have been signed into law, with at least two more states close to enactment.[4]

These three laws join the Virginia Consumer Data Protection Act, or VCDPA,[5] the California Consumer Privacy Act, or CCPA,[6] the Colorado Privacy Rights Act, or CPA,[7] Connecticut's Public Act No. 22-15, or CTPA,[8] and the Utah Consumer Privacy Act, or UCPA,[9] in the U.S. state comprehensive consumer privacy law framework.

A common thread among several comprehensive state privacy laws is the requirement for controllers to conduct and document a data protection impact assessment, or DPIA, for various data practices, including targeted advertising, consumer profiling and sensitive data processing.

"Controller" is generally defined as an entity that, alone or jointly with others, determines the purpose and means of processing personal data.[10]

Gating assessments of all new or modified data practices can serve the dual purpose of updating data inventories and notices and confirming if full assessments are necessary.

Out of the comprehensive state consumer privacy laws mentioned above, Virginia, Connecticut, Colorado, Indiana and Tennessee's laws have DPIA requirements, with only Utah and Iowa's privacy laws containing no requirements on this subject.

The CCPA will also require DPIAs, subject to future rulemaking detail.

In addition, other privacy laws may also apply and obligate DPIAs, including the California Age-Appropriate Design Code Act, or CAADCA,[11] and New York City's Local Law 144.[12]

The following is a summary of basic requirements under the six comprehensive state consumer privacy laws, along with the requirements under CAADCA and Local Law 144.

Comprehensive Consumer Privacy Laws

VCDPA, CTPA, ICDPA and TIPA

The DPIA requirements under Virginia, Connecticut, Indiana and Tennessee law are almost identical.

Controllers subject to these laws must conduct and document a DPIA 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,[13] and other processing activities that present a heightened risk of harm.

In each DPIA, 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 must 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 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 under the CTPA, on July 1, 2024, under the TIPA, and Jan. 1, 2026, under the ICPDA.

CPA

Colorado's requirements under the CPA and its final rules are the most extensive.[14]

Like the above states, controllers subject to the CPA must conduct DPIAs 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.[15]

Assessments must conduct a risk-benefit analysis, including a discussion of safeguards and measures taken to offset the risks.

Unlike the above states' broad requirements, the CPA final rules 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. Among these are data security and compromise considerations.

In addition, the CPA final rules explicitly require that the assessment involve all relevant internal actors from across the company's organizational structure, as well as relevant external parties, where appropriate, to identify, assess, and address the data protection risks.

While the other states do not require this level of detail, the inquiries are reflective of the general considerations mandated by the other states.

Once the requirement to conduct a DPIA 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.

CCPA

The details of DPIA requirements have not yet been addressed under the CCPA, which calls for details to be determined in rulemaking.

Thus far, the California Privacy Protection Agency, or CPPA, is considering basing its DPIA rules on European Data Protection Board, or EDPB, guidelines[16] 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 guide the development of a multistate assessment program, and can be treated as best practices even if not fully adopted by California.

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 DPIA, it must justify and document the reasons for this decision.

At a minimum, under the EDPB guidance, DPIAs 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, along with other suggested additions and mandatory factors to consider.

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.

For all of the above laws, each applicable processing activity must have its own DPIA, but a single assessment can cover comparable processing activities.

Similarly, each law provides that if a controller conducts a DPIA to comply with one state law, that assessment will satisfy the requirements established by the other state laws if it is reasonably similar in scope and effect to those state law requirements.

What is not explicitly mandated by these state laws, but is inherent is the risk analysis they require, is a methodology for scoring risk — such as by likelihood and severity — and standards of risk tolerance and prioritization tied to corporate philosophy and brand identity as to social responsibility and ethical processing.

Accordingly, an effective privacy, data protection and information governance program and policy plan — which we will refer to collectively as a data governance program — can establish not only how assessments are to be conducted and by whom, but also the standards and frameworks that should be applied.

Assessments are a part of data governance, but the program plan sets how to conduct assessments and make assessment decisions. Accordingly, they go hand in hand.

The CPA finals rules' explicit requirement that assessments consider security and include input by all internal stakeholders, which are implicitly required under the other state law assessment provisions, also calls for an enterprisewide data governance program for which privacy and legal are part, but not the entirety, of the program participants.

The TIPA bill had proposed to require such a written plan, to be developed and operated consistent with the National Institute of Standards and Technology Privacy Framework and certain scope and scale considerations, but as passed makes such a program plan voluntary, while offering a potential affirmative defense to TIPA violations if a controller has a written privacy program plan that meets certain requirements.

California Age-Appropriate Design Code Act

Under the CAADCA, businesses that provide an online service, product or feature likely to be accessed by children — defined as consumers under 18 years of age — must complete a DPIA before such online service is offered to the public, beginning on July 1, 2024.

The DPIA must identify the purpose of the online service, how it uses children's personal data and the risks of material detriment to children that arise from the data management practices of the business.

Specifically, the DPIA must address:

- Whether the design of the online service could harm children, including by exposing children to harmful, or potentially harmful, content on the online service;

- Whether the design of the online service could lead to children experiencing or being targeted by harmful, or potentially harmful, contacts on the online service;

- Whether the design of the online service could permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct on the online service;

- Whether the design of the online service could allow children to be party to or exploited by a harmful, or potentially harmful, contact on the online service;

- Whether algorithms used by the online service could harm children;

- Whether targeted advertising systems used by the online service could harm children;

- Whether and how the online service uses system design features to increase, sustain, or extend use of the online service by children, including the automatic playing of media, rewards for time spent and notifications; and

- Whether, how, and for what purpose the online service collects or processes sensitive personal data of children.

Businesses must create a timed plan to mitigate or eliminate risks identified before the online service is accessed by children.

The California attorney general can make written requests to see specific DPIAs or a list of all DPIAs the business has completed, and the business must comply within three to five business days.

NYC Local Law 144

New York City's Local Law 144 addresses the use of automated employment decision tools, which are used to screen and score job applicants and employees applying for promotions.

Local Law 144 requires employers and employment agencies to conduct a bias audit within one year of using an automated employment decision tool.

For automated employment decision tools that select or classify individuals into groups, the bias audit must calculate the selection rate for each category — defined as any component 1 category required to be reported by employers pursuant to Title 42 of the U.S. Code, Section 2000e-8, including sex, race and ethnicity for each occupational position — and calculate the impact ratio for each category.

For automated employment decision tools that score applicants or candidates, bias audits must calculate the average score for individuals in each category and calculate the impact ratio for each category.

Results of bias audits must be publicly available on the employer's or employment agency's website. Local Law 144 will likely be enforced beginning on July 5, 2023.

The final rule helpfully provides charts and formulas to reference when conducting bias audits. Additional laws regulating artificial intelligence are under consideration globally, most of which call for data privacy and ethical processing assessments. AI voluntary frameworks do likewise.

Further, AI assessments can also consider other important issues like intellectual property, usage controls, confidentiality and reliability.

Data Governance Must Evolve to Meet New Requirements

The requirements for the content of assessments can be extensive, and new laws are being passed quickly.

In addition, businesses subject to these laws should consider a data governance and ethical processing program policy and framework that has standards to apply to making assessment decisions, and procedures for conducting assessments.

Many controllers are still struggling with setting up basic elements of privacy compliance and info gov — data mapping and data subject notices and rights request programs — and have not yet wholistically addressed data governance.

New assessment requirements present the opportunity, if not practically the necessity, to do so.

Alan Friel is a partner and chair of the global data practice at Squire Patton Boggs LLP.

Sasha Kiosse is an associate at the firm.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Iowa Code Chapter 715D.

[2] Ind. Code 24-15.

[3] Tenn. Code Ann. § 47-18-3201.

[4] See Montana Consumer Data Privacy Act, SB0384 (2023); Florida's An Act Relating to Technology Transparency, SB0262 (2023). Both bills have been enrolled.

[5] Va. Code § 59.1.

[6] Cal. Civ. Code § 1798.100.

[7] C.R.S. 6-1-1301.

[8] CT P.A. 22-15.

[9] Utah Code § 16-61-101.

[10] See generally CT P.A. 22-15, § 1(8); Va. Code § 59.1-571; C.R.S. 6-1-1303(7); Ind. Code 24-15, ch. 2 § 9; Tenn. Code Ann. § 47-18-3201(8). In California, under the CCPA and CAADCA, the term "business" is used instead of "controller." Cal. Civ. Code § 1798.140(d); Cal. Civ. Code § 1798.99.30 (applying definitions from CCPA).

[11] Cal. Civ. Code § 1798.99.28.

[12] New York City Local Law 144.

[13] Specifically, DPIAs are necessary when the 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." See generally CT P.A. 22-15, § 8(a); Va. Code § 59.1-576(A); Ind. Code 24-15, ch. 6 § 1(b); Tenn. Code Ann. § 47-18-3206(a).

[14] 4 CCR 904-3.

[15] The same factors are considered when profiling presents a reasonably foreseeable risk as under CTPA, VCDPA, ICDPA, and TIPA. C.R.S. 6-1-1309(2).

[16] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, European Data Protection Board.