SQUIRE PATTON BOGGS

# US Regulators Lift the Curtain on Data Practices With Assessment, Reporting and Audit Requirements

March 2024

**Authors:**

**Alan Friel**, **David Manek**, **Sasha Kiosse**, **David Farber** and **Colleen M. Yushchak**[1]

## Originally Published in ALM's *Cybersecurity Law and Practice,* March 2024

California enacted the California Consumer Privacy Act (CCPA) in 2018, which was the first of its kind in the US and drew inspiration from Europe's General Data Protection Regulation (GDPR). Following California's lead, other states, including Colorado, implemented their own laws and regulations. California further strengthened its legislation in 2020 through a ballot initiative known as the California Privacy Rights Act (CPRA).

Unlike the GDPR, the first generation CCPA was light on affirmative due diligence requirements and many companies designed data privacy and protection programs that were little more than window dressing (e.g., privacy policies and a consumer rights request process). In the second generation of state consumer privacy laws and regulations, as well as in recent laws pertaining to the privacy of minors (such as in California and Connecticut), numerous states require affirmative due diligence and a structured approach for conducting and documenting risk assessments, as well as associated remediation. The assessment documentation must be available for review by regulators, and the CPRA requires risk assessments to be filed with the state, a requirement that is currently under consideration in a condensed form with certification by the executive officer. This means that companies subject to the applicable state privacy laws need to develop or refine their data inventory and assessment practices as a top priority in 2024 to be prepared for the coming enforcement of these requirements.

## How Did We Get Here?

Companies subject to the consumer privacy regimes in California (CCPA), Colorado (CPA), Connecticut (CTPA) and Virginia (VCDPA) are now required to conduct and document data protection assessments prior to engaging in certain types of data processing. At least eight additional state laws that go into effect in 2024 and 2025 have similar requirements. Most notably, assessments are required if the processing is deemed "high risk," which specifically includes, without limitation, processing for targeted advertising, profiling/automated decision-making (ADM), processing of sensitive personal data and sale of personal data. Since these requirements are inspired by the GDPR, companies should consider guidance from the European Data Protection Board (EDPB) on what might be considered high-risk processing, and how to analyze risk.

So far, only Colorado has promulgated regulations or issued guidance regarding what needs to be in assessments and how they should be conducted and documented, but California is currently developing its own rulemaking that it has stated seeks to be compatible with Colorado and reflect EDPB guidance.

Some states, like Virginia and Connecticut, are not likely to detail what will be required for assessments. However, others, like New Jersey (the latest state to pass a consumer privacy law), contemplate rulemaking. Some currently effective state privacy laws like the Utah Consumer Privacy Act and the Iowa Consumer Data Protection Act do not specifically require assessments, but the data minimization and purpose limitation provisions of those laws make assessments practically necessary. Similarly, the newly enacted Washington My Health My Data Act (MHMDA) does not require assessments, but its requirement to establish, implement and maintain administrative, technical and physical data security practices that, at a minimum, satisfy reasonable standards of care within the industry suggest a practical need for using assessments. Connecticut's version of MHMDA requires formal assessments. The California Age-Appropriate Design Code Act (AADCA) requires assessments, as does Connecticut's version of that law. In addition, Colorado, Virginia, Tennessee, Indiana, Texas, Montana, Florida, Oregon, Delaware, New Jersey and New Hampshire treat children's personal data, and in some cases other minors' personal data, as sensitive information, the processing of which requires a risk assessment. The same is true of biometrics in California, Connecticut, Colorado, Virginia, Tennessee, Indiana, Texas, Montana, Florida, Oregon, Delaware, New Jersey and New Hampshire. Regardless of whether US privacy laws explicitly require assessments, their growing complexity and evolving best practices practically necessitate them.

A handful of states will likely take the lead in fleshing out what an assessment program should look like. Colorado finalized regulations on assessments on March 15, 2023, and they are effective as of July 1, 2023. In December 2023, the California Privacy Protection Agency (CPPA) published revised draft regulations on risk assessments, which were updated in February 2024 (CA Draft Regs), and set to be voted on by the CPPA Board on March 8, 2024. If approved by the CPPA Board, they will advance to public comment and formal rulemaking. They largely reflect, and add to, Colorado's requirements. When combining these resources with EDPB guidance, there is enough meat on the bones for companies to be able to start operationalizing data practice assessments, which will be no small task for many companies.

## What Is a Data Risk Assessment and What Is Its Purpose?

A data risk assessment gathers and documents key information regarding a current or contemplated data practice. It is essentially a due diligence process that inventories the data and establishes the associated processing activities and purposes – collection, use, storage, disclosure and protection. Once key information is documented, a privacy and/or legal professional assesses whether the benefits of the processing purposes outweigh the risks to the data subjects and other impacted individuals.

1 Alan Friel is the chair of our Data Privacy, Cybersecurity & Digital Assets Practice based in Los Angeles. The other authors are privacy professionals at Ankura Consulting Group. The authors thank associate Sasha Kiosse for her research assistance.

They also assess if the processing purposes are consistent with both the collection purposes and the reasonable expectations of the consumer. Lastly, they validate if the processing will comply with legal limitations and obligations. That said, this is not just a legal compliance risk reduction exercise. Clearing the ability to commercialize personal data in the manners desired legally, ethically and without business interruption is key to maximizing digital asset value. In addition, the initial due diligence process enables companies to keep data inventories and maps current, which is essential to effective data management and information governance.

## When Is an Assessment Necessary or Otherwise Advisable?

Applying the highest watermark of what it would take for a single program to comply with all the applicable state laws, and applying best practices, assessments should be undertaken if any of the following activities are present regarding personal data it controls, in whole or in part:

- Processing sensitive data
- Processing for targeted advertising
- Selling personal data
- Sharing personal data for cross-context behavioral advertising
- Processing personal data for high-risk profiling (e.g., where it could impact access to essential goods or services or impact rights)
- Using automated decision-making technology for:
  1. A decision that produces legal or similarly significant effects concerning a person
  2. Profiling a person acting in their capacity as an employee, job applicant, independent contractor or student
  3. Profiling a person in a publicly accessible place
  4. Behavioral advertising (including first party)
- Processing the personal data of children or other minors
- Processing data on a large scale
- Processing personal data to train AI or ADM technology
- Matching or combining data sets in a way that would exceed the reasonable expectations of the data subjects
- Innovative use or use of new technology
- If the processing itself prevents consumers from exercising a right or using a service
- Use of cookies or other tracking technologies
- When a security incident would trigger an obligation to notify data subjects or the government

At the same time an inquiry is made to determine if any of these high-risk activities are present, necessitating a full risk assessment, data inventories can be refreshed and compliance (e.g., notice at collection, ability to apply consumer rights like deletion requests, etc.) with respect to processing that is not high risk can be confirmed. Accordingly, initial diligence is recommended for all new, changed and ongoing personal data processing practices.

## What Is Required to Be Included in an Assessment?

Once the need for a risk assessment is identified, a meaningful risk analysis should be conducted that:

1. Identifies and describes the risks to the rights of data subjects and others associated with the processing
2. Considers transparency
3. Documents technical and organizational remedial measures considered and taken to address and offset those risks
4. Reviews the benefits of the processing and demonstrates that the benefits of the processing outweigh the risks offset by safeguards in place or to be taken, taking into account the scope of risk presented, the size of the company, the amount and sensitivity of personal data processed, the nature of the personal data processing activities subject to the assessment and the practicalities of available safeguards

Again, applying a high watermark, assessments should include the following information to inform the risk/benefit analysis:

1. A summary of the processing activity
2. Identification of the personal data involved in the processing activity, including identification of sensitive data and the sources of the data
3. The context, nature purposes and operational elements of processing
4. A risk-benefit analysis of the processing activity
5. Identification of potential risks and harms and description of measures taken to address risks, as well as the potential benefits of the processing activity
6. A list of internal and external actors involved in the processing activity, including all data recipients
7. A description of notices and choices to be given to data subjects, particularly as required by applicable law
8. Other specific requirements enumerated in the state laws or the Colorado or California regulations, particularly regarding Automated Decision Making (ADM)/profiling and processing of sensitive data; for example, regarding CA AADCA, there are additional assessment requirements before an online service, product or feature likely to be accessed by minors is offered to the public

While US privacy laws do not mandate a particular methodology for analyzing risk and impact, they do call for a risk/benefit balancing and, in some cases, the consideration of very specific issues, such as for ADM the potential for bias and error. One way to evaluate risk, recommended by the UK Information Commissioner's Office, is by ranking severity and likelihood of harm, which can be plotted on an x/y axis. Numerical scoring and heat mapping can help illustrate risk but should not be overly relied upon. A finding of high severity and high likelihood would be the highest risk type of activity, which would require the addition of safeguards to lower the level of severity and/or likelihood to an acceptable level. For instance, violating data subject rights under applicable law would score very high as to severity of harm, but legal compliance safeguards should be able to reduce the likelihood of that harm to near zero. A similar analysis can be applied to issues of data security and intrusion upon reasonable expectations of privacy. Some practices may not be capable of sufficient risk reduction through safeguards and remediation and will need to be prohibited, while others may be approved with conditions designed to mitigate risk of severity and likelihood of harm and otherwise to comply with applicable legal obligations.

Whether or not a scoring system is utilized, there should be a policy standard against which decisions are made. Such a standard can be articulated in a privacy program plan and in a responsible AI policy. Such plans and policies can be built around frameworks such as NIST (see the NIST Privacy Framework and the NIST AI Risk Management Framework). Tennessee's new privacy law offers a potential safe harbor to violations, if a controller maintains a written privacy program plan that meets certain adequacy requirements and is consistent with NIST or other similar privacy frameworks. A more simple privacy framework that has influenced data privacy and information governance laws and best practices worldwide, including the new generation of US privacy laws, is the US government's Fair Information Practice Principles (FIPPs), which can be combined with "privacy by design" to implement the FIPPS principles of transparency, individual participation, authority, purpose specification and use limitation, data minimization, quality and integrity, access and amendment and security and accountability that are becoming codified as part of evolving legal regimes.

## Who Is Responsible for Conducting and Approving Assessments?

Assessments should be conducted by a professional versed in the company's privacy program plan and associated policies, as well as applicable law. That individual can make the decision to accept, reject or modify the assessed activity. This need not necessarily be done by a lawyer, but it is advisable to seek guidance from legal counsel with respect to compliance questions. The advice of legal counsel that guides the assessment process and conclusions, as maintained as legal work product and attorney-client communications, should be privileged even if the final business record of the assessment documentation may not be. The CA Draft Regs include a requirement for the company's board to be informed of assessment findings and an executive officer to certify assessment findings and recommendations. This raises assessment oversight responsibilities to the board and C-suite.

## When Must Assessments Be Conducted?

Timing for conducting and documenting assessments varies by state. In Virginia, Connecticut, Colorado and Florida, assessment requirements are already in effect, with Virginia requiring assessments for applicable processing activities conducted or generated after January 1, 2023, and Connecticut, Colorado and Florida requiring assessments for processing activities "conducted or generated after" (in Connecticut and Colorado) or "generated on or after" (in Florida) July 1, 2023. Assessment requirements are effective in Oregon, Tennessee and New Hampshire in 2024, with Oregon requiring assessments for processing activities that occur on or after January 1, 2024, and Tennessee and New Hampshire requiring assessments for processing activities created or generated "on or…" (Tennessee) after July 1, 2024. The rest of the states' assessment requirements go into effect in 2025 and 2026; Texas and Montana provide for assessments as of January 1, 2025, with Texas requiring assessments for processing activities "generated after" that date and Montana requiring assessments for processing activities "created or generated after" that date; New Jersey requires assessments for processing activities that involve personal data acquired on or after January 16, 2025; Delaware requires assessments for processing activities created or generated on or after July 1, 2025; and Indiana requires assessments for processing activities created or generated after December 31, 2025.

As noted above, many of the state privacy laws contain the language "created or generated" when providing timing requirements. There is ambiguity whether processing activities "created or generated" on or after a certain date include activities that began prior to that date and are ongoing. However, the word "generated" can be interpreted to include ongoing activities; thus, it is recommended to conduct assessments for such ongoing activities under the state laws to remain compliant.

As for California, the CA Draft Regs pertaining to risk assessments have not, as of the publication date of this article, yet been enacted, and it is not yet clear what the timing requirements for assessments will be. The draft discussion regulations currently provide that assessments are required "for any processing activity … that the business initiated prior to the effective date of these regulations and that continues after the effective date of these regulations … within 24 months of the effective date of these regulations." It is unknown when the draft discussion regulations will be finalized and ready for approval.

California's AADCA requires data protection assessments before any new online services, products or features likely to be accessed by children are offered to the public. This requirement goes into effect when AADCA becomes effective on July 1, 2024. However, on September 18, 2023, a federal court granted an injunction to prohibit the enforcement of AADCA on the grounds that it likely violates the First Amendment of the US. The California Attorney General filed a notice of appeal in October 2023 and an appellant brief in December. It is unclear how the appellate court will rule on AADCA and whether it will go into effect on July 1, 2024.

## When Should Assessments Be Updated and How Long Should They Be Maintained?

Again, applying the highest watermark of what it would take for a single program to comply with all of state laws, assessments should be updated periodically (annually for profiling in Colorado and potentially every three years regardless of processing type in California) and considering the level of risk and any changes made throughout the processing activity's life cycle. Under CA AADCA, assessments must be biennially reviewed and updated and must be maintained for as long as the online service, product or feature is likely to be accessed by minors.

Assessments should be stored throughout the life cycle of the processing activity and for at least three years after its end (California is considering five years).

## How Can Assessments Be Operationalized and Who Should Be Responsible for What?

The first phase in operationalizing an assessment process is to develop a privacy impact assessment workflow.

**Identifying use cases** – To identify the use case for when an assessment needs to be completed, organizations should first review artifacts previously created to support their privacy compliance program, such as their data map or records of processing activities. Next, organizations that maintain modern vendor risk management programs can also utilize the output from vendor due diligence assessments to identify vendors, systems and processes that may require further assessment. Lastly, the privacy, legal or compliance team responsible for identifying assessment use cases should consider a quarterly (or more frequent) meeting with their development team to review new initiatives, changes to existing processes, product changes and new releases.

**Gating assessment** – An important aspect in developing a functioning assessment workflow is to limit the number of questions that need to be answered to only those questions that are relevant or required. To accomplish this, organizations should first consider issuing a gating assessment that includes a set of basic questions focused on determining if a full assessment is needed. The gating assessment is focused on identifying processing activities, assets and third parties involved in the processing of personal information. The gating assessment also includes questions to assess whether the processing of personal information triggers a regulatory obligation to conduct a full assessment such as processing sensitive data, minors' data, selling of personal data or processing for targeted advertising. The purpose of the gating assessment to determine if a full assessment is needed and what subcomponents of the full assessment are to be introduced into the assessment process.

**Full assessment and subcomponents** – If the results of the gating assessment point to the need to conduct a full privacy impact assessment, a good practice is to trigger optional additional assessment sections as needed to further assess activities relating to artificial intelligence, processing of children/minor's data, consumer health information or biometric information. Lastly, and most importantly, the assessment will need a section to document a remediation plan to address identified risks.

**Leveraging technology** – Many organizations are leveraging assessment technology to support automating certain aspects of their assessment workflow. Some benefits to using privacy management technology to support the assessment process include the ability to create customized and user-friendly assessments that utilize conditional logic to better streamline the process. Such tools also contain workflow functionality to automatically launch additional assessments based on responses in the gating assessment.

The use of privacy management technology can support integrations between the privacy impact assessment process, data inventory and third-party risk management process. For example, an assessment question that is asked in the initial third-party risk management assessment be prepopulated in follow-on assessments so that organizations can more easily leverage information that has already been collected.

Privacy management technology can also support collaboration between business owners via custom workflows in the instances where multiple stakeholders need to be considered in the assessment process.

## When Must Assessments Be Filed With or Made Available to the Government?

Generally, a company should be prepared to disclose assessments to the respective state's regulator upon request, which should be subject to confidentiality protections. The CCPA gives the CPPA authority to require assessments to be filed with the state. Currently, the CPPA is discussing requiring filing only summaries of assessments. Companies may also want to create a summary of a completed assessment to share with customers, particularly in a business-to-business due diligence context.

## What About Cybersecurity?

In addition to assessment requirements, state privacy and data protection laws include provisions for cybersecurity audits. Many of the laws offer controllers a right to conduct reasonable audits of processors, and California and Colorado obligate controllers to review their vendors' security practices. The CA Draft Regs include a proposed audit scope and establish a process to ensure that audits are thorough and independent and that summaries of all audits are filed with the agency. These requirements will be detailed in a further article.

## Conclusion

In conclusion, the assessment and audit requirements of this new generation of state data protection laws will force US companies to move beyond mere window dressing (e.g., privacy policies and consumer rights request mechanisms) and instead require them to develop fulsome data protection programs. If California follows through on requiring assessment and audit summaries to be certified and filed with the state, regulators will be able to easily see which companies are not complying with risk assessment requirements.

## Contact

**Alan L. Friel**
Partner and Chair, Global Data Privacy, Cybersecurity and Digital Assets Practice
T +1 213 689 6518
E alan.friel@squirepb.com

**2023 *Global Data Review* ranked "Elite" and top 20 law firm for data.**

**Subscribe to our blog Privacy World.**