

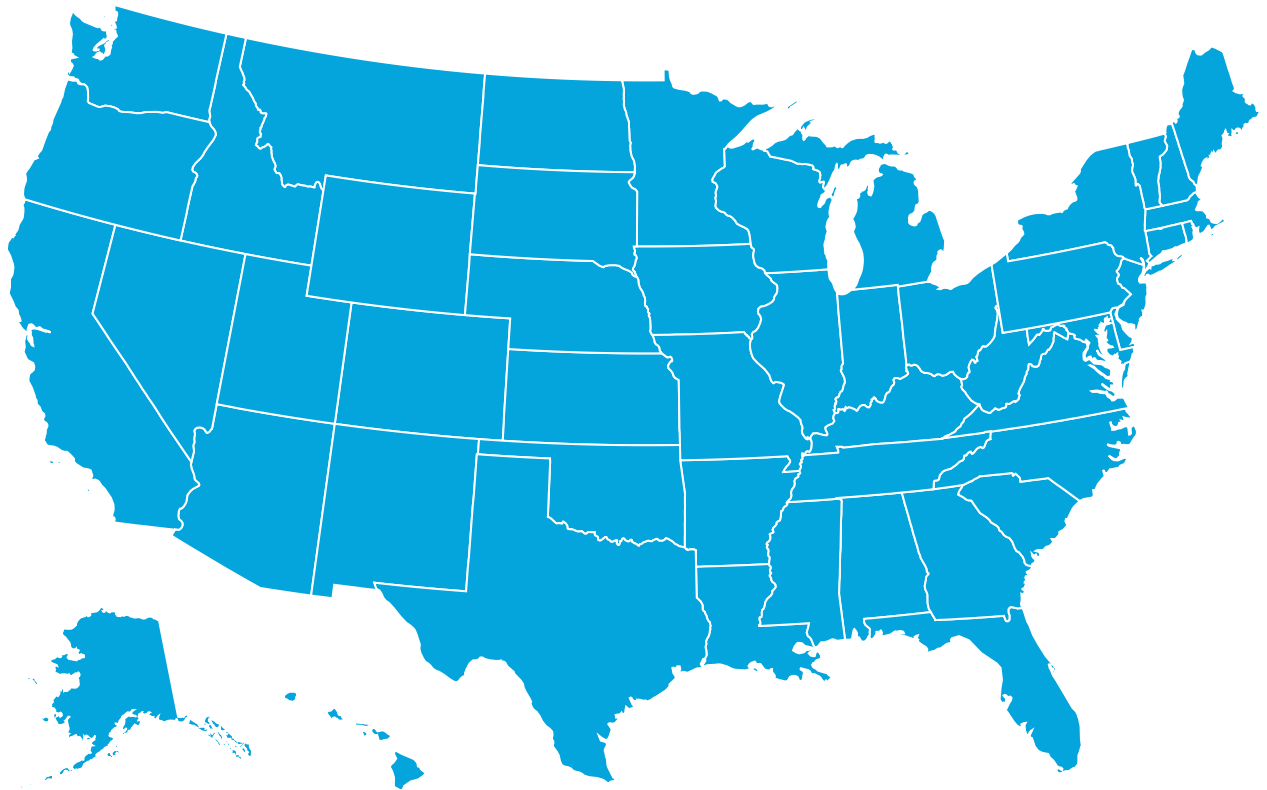


Centre for Information Policy Leadership

HUNTON ANDREWS KURTH

Comparison of U.S. State Privacy Laws

Data Protection Assessments



February 2024

Comparison of US State Privacy Laws: Data Protection Assessments

EXECUTIVE SUMMARY

The ever-growing number of privacy laws enacted by state legislatures and the lack of a uniform federal standard have left organizations in the United States wrestling with inconsistent legal obligations regarding the collection and use of personal data. The Centre for Information Policy Leadership (“CIPL”) is writing a series of papers to describe the compliance challenges stemming from these factors, and to offer recommendations to policymakers who may be considering changes to existing laws or the introduction of new ones. This first paper in the series addresses **data protection assessment** requirements. It addresses the difficulties organizations face in light of divergent rules and urges state lawmakers to promote interoperability and convergence moving forward.

Specifically:

- Organizations need **consistency in terminology and definitions** in order to build cohesive and effective data protection assessment and compliance programs.
- Organizations strive to build comprehensive privacy programs—of which data protection assessments are a fundamental building block—to satisfy important compliance obligations across a number of US and global jurisdictions and to ensure consistent protections for their customers. Many organizations use the requirements of the **EU General Data Protection Regulation (“GDPR”) as the highest common denominator**. But as new state laws introduce additional elements, the need to make a variety of *ad hoc* amendments to an already comprehensive assessment renders an otherwise streamlined approach inefficient and unworkable.
- Responsible organizations **meaningfully engage with a range of internal and external organizations (including auditing companies) to conduct comprehensive data protection assessments, but the form and substance of the engagement varies from organization to organization**. Regulators and lawmakers should incentivize meaningful engagement relating to effective risk assessments as a best practice, but not prescribe particular methods or elements.
- If, however, organizations are required to **share data protection assessments with regulators or enforcement bodies proactively on a regular basis, in detail or summary form, is unnecessary and burdensome** in a dynamic regulatory and technological landscape. Instead, organizations should be required to maintain records of their data protection assessments and be ready to produce them to appropriate authorities upon request in the event of an investigation or other enforcement action.
- To the extent organizations are required to provide regulators with a summary version of a data protection assessment, regulators should provide **clear guidance on the elements to include in such a summary** to ensure consistency between summaries, as well as to preempt potential questions about apparent discrepancies or potential claims of misrepresentation relating to a comparison between a full, underlying data protection assessment and the summary of it.

- Existing data protection assessment requirements should be written and/or interpreted as much as possible to **enable organizations to use one assessment to satisfy the requirements in most or all states and to make them interoperable between jurisdictions.**

BACKGROUND AND SCOPE

With an ever-growing number of privacy laws in the US enacted by state legislatures,¹ companies with limited budgets and limited resources are seeking ways to synthesize requirements and harmonize compliance obligations across jurisdictions. CIPL² has initiated a project to identify areas of alignment and divergence between state laws, and to examine the compliance challenges companies face as a result of the divergences. Our goal is to help state law and policy makers in the US advance the principles of privacy and data protection in a more consistent and manageable way.

Congressional action on privacy also remains important. The politics around federal privacy legislation are complex, especially with respect to issues such as private right of action and pre-emption. Nevertheless, the increasing number of state laws may provide motivation for Congress to develop a federal bill that builds upon the points of convergence across state privacy laws and resolves problematic inconsistencies among them. CIPL hopes that our project can also usefully inform the preparation of federal legislation.

The present paper analyzes **data protection assessment requirements** set forth in comprehensive state privacy laws.³ To benchmark them against the currently dominant global standard on this issue, we also compare them to the risk assessment requirements found in the EU General Data Protection Regulation (“GDPR”). In our analysis, we use the term “data protection assessment” to denote a range of fundamentally equivalent and interchangeable concepts found in diverse legal frameworks. This includes, but is not limited to, “data protection impact assessments” (“DPIAs”), “privacy impact assessments” (“PIAs”) and “risk assessments” or “privacy risk assessments.” We use the term “data protection assessment” because it is the most prevalent term found in comprehensive state privacy laws, but our

¹ As of February 8, 2024, the following states adopted their own comprehensive privacy laws: California (“CPRA” or “the CCPA as amended”), Virginia (“VCDPA”), Colorado (“CPA”), Utah (“UCPA”), Connecticut (“CTDPA”), Delaware (“DOPPA”), Iowa (“ICDPA”), Indiana (“ICDPA”), Tennessee (“TIPA”), Montana (“MCDPA”), New Jersey (“NJCPA”), Florida (“FDBR”), Oregon (“OCPA”) and Texas (“TDPSA”). We include Florida in our list of comprehensive laws, although some sources do not count it due to its applicability to a limited set of entities. We also include New Hampshire in our analysis because the state legislature passed Bill SB 255 (“NHPA”) on January 18, 2024.

² CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL’s mission is to engage in thought leadership and develop best practices that ensure effective privacy protections and the responsible use of personal information in the modern information age. Please see CIPL’s website at www.informationpolicycentre.com. Nothing in this paper should be construed as representing the views of any individual CIPL member company or Hunton Andrews Kurth, nor does anything in this paper constitute legal advice.

³ For the purpose of this paper, “comprehensive state privacy laws” means state data privacy regulations governing the rights of consumers and imposing obligations on covered entities. These regulations generally apply only to non-governmental organizations meeting certain thresholds. They commonly exclude employment-related data (except in California) and provide exemptions, such as for non-profits or certain regulated industries subject to other regulations like the GLBA and HIPAA.

analysis aims to capture assessments, regardless of terminology, which are designed to gauge and mitigate the risks associated with the processing of personal data.

We recognize that certain specialized, non-comprehensive data privacy laws may have similar assessment requirements that could relate to our present analysis. For example, the currently blocked California Age-Appropriate Design Code Act requires businesses offering online services, products or features likely to be accessed by children to conduct data protection impact assessments.⁴ The present analysis, however, focuses on data protection assessment requirements found in comprehensive state privacy laws.

SPECIFIC ISSUES

A. Terminology for Key Concepts

The diverse terminology and definitions used by different states for similar or identical concepts creates confusion and unnecessarily complicates effective compliance for organizations. This applies for data protection assessments and other elements of privacy laws.

For example, in the comprehensive privacy laws adopted by most states, there is a consensus that the processing of “sensitive data” heightens the risk of harm to consumers, necessitating a specific data protection assessment. However, each state’s law introduces unique definitions for sensitive data. California and New Jersey, for example, define sensitive personal information more expansively (and more specifically) than other states. These two states define the concept to include account log-in details, financial account information, debit or credit card numbers combined with any requisite security or access code, passwords or credentials allowing account access.⁵ California also includes the contents of a consumer’s communications when the business is not the intended recipient, government ID information (e.g., social security, driver’s license, state ID or passport number), philosophical beliefs and union membership.⁶ But even where California and New Jersey align with most states, such as in classifying precise geolocation data as sensitive, an exception can be found elsewhere: Colorado’s privacy law does not include geolocation data within its definition of sensitive data.⁷

Such state-by-state differences create unnecessary complexities in organizations’ privacy compliance and management programs, which typically strive toward one uniform national or even global approach. Such differences not only undermine effective compliance, but also risk leaving US consumers with different levels of privacy protections depending on where they happen to be located.

⁴ Cal. Civ. Code Section 1798.99.31(a)(1), available [here](#). Additional information about the California Age-Appropriate Design Code can be found [here](#).

⁵ Section 1798.140(ae) of the California Consumer Privacy Act and Section 1 of the New Jersey Bill 332.

⁶ *Ibid.*

⁷ Section 6-1-1303 (24) CPA. Note that “precise geolocation” is defined differently in some states, particularly concerning the distance that is considered to be “precise”. For example, in California, “precise geolocation” refers to locating a consumer within a geographic area equal to or less than the area of a circle with a radius of 1,850 feet, whereas in New Jersey, the precision and accuracy are within a radius of 1,750 feet.

FINDINGS & RECOMMENDATIONS

- Adopt consistent terminology and definitions across state laws to facilitate uniformity in data protection assessments and data privacy protections for consumers, regardless of state of residence. States use different terms to address similar concepts, such as the risk threshold to trigger assessments (e.g., heightened risk, significant risk), as well as different definitions of key terms such as “sensitive personal data” or “profiling.” These differences pose challenges for compliance, as organizations seek to parse out which differences are substantively meaningful, and which have little operative impact. Greater consistency and clarity across key definitions will enable organizations to focus on building and operating meaningful protections for data subjects rather than attempting to differentiate compliance based on differences that sometimes are clear and meaningful, sometimes subtle and unclear and sometimes potentially non-substantive.

B. Threshold for Data Protection Assessments

Most Common Approach: Heightened Risk of Harm—Like the GDPR, the privacy laws of many US states⁸ explicitly require a data protection assessment for processing activities that meet a certain risk threshold. The majority of states⁹ identify a “**heightened risk of harm to consumers**” as the applicable threshold and prescribe the following processing activities as illustrative examples:

- (i) the sale of personal data,
- (ii) the processing of sensitive data;
- (iii) targeted advertising;¹⁰
- (iv) profiling that presents a reasonably foreseeable risk of substantial injury to consumers (e.g., unfair or deceptive treatment, financial, physical or reputational injury); and
- (v) other processing activities presenting heightened risk of harm to consumers.¹¹

In the absence of regulatory guidance, the heightened-risk-of-harm standard delegates the identification of “other” heightened risk activities to organizations, typically accomplished through an initial risk triage process.

Other Approach: Reasonably Foreseeable Risks of Harm in Utah & Iowa—Utah and Iowa do not explicitly include a data protection assessment requirement in their privacy laws, but both states imply such a requirement by requiring organizations to “establish, implement, and maintain reasonable administrative,

⁸ Specifically, California, Colorado, Connecticut, Delaware, Florida, Indiana, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas and Virginia.

⁹ Colorado, Connecticut, Delaware, Florida, Indiana, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas and Virginia.

¹⁰ Interestingly, in the context of targeted advertising, Colorado recognizes a heightened risk of harm in circumstances where the advertising presents a “reasonably foreseeable risk of substantial injury” to consumers. See Section 6-1-1309(2)(a) CPA.

¹¹ Section 6-1-1309 CPA, Section 8(a) CTDPA, Section 12D-108(a) DOPPA, Section 16-501-713 of FDBR, Chapter 6-Section 1 ICDPA, Section 9 MCDPA, Section 507-H:8(I) NHPA, Section 9(c) NJCPA, Section 8(1) OCPA, Section 47-18-3206 TIPA, Section 541-105 TDPSA and Section 59-1-576 VCDPA.

technical and physical data security practices *designed to reduce reasonably foreseeable risks of harm to consumers*” relating to the processing of personal data.¹² Indeed, reducing a reasonably foreseeable risk of harm cannot be accomplished without first performing a risk assessment.

Other Approach: Risk Thresholds in California and EU GDPR—The risk thresholds for conducting a data protection assessment in California (i.e., “significant risk to consumers’ privacy”¹³) and the GDPR (i.e., “high risk to the rights and freedoms of natural persons”¹⁴) differ from the threshold followed by the majority of states (i.e., heightened risk of harm to consumers) and specifically prescribe certain risks to be avoided.

Specifically, California’s Draft Risk Assessment Regulations list the following activities as posing significant risks to consumers’ privacy:

- (i) the sale or sharing of personal data;
- (ii) the processing of sensitive data;
- (iii) the use of automated decision making (“ADM”) technology in furtherance of a decision that results in access to essential goods, services and opportunities (e.g., financial services, housing, insurance, educational enrollment, employment, criminal justice, healthcare services);
- (iv) the processing of known children’s data (below 16 years old);
- (v) the use of technology to monitor employees, independent contractors, job applicants or students;
- (vi) the use of technology to monitor consumers’ behavior, location, movements or actions in publicly accessible places; and
- (vii) training AI or ADM.¹⁵

Like California, the GDPR lists specific instances where a data protection assessment is mandatory; it identifies the following activities as likely to present a high risk to the rights and freedoms of natural persons:

- (i) where there is a systematic and extensive evaluation of personal aspects based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or otherwise significantly affect the individual;
- (ii) where there is large-scale processing of special category data; or
- (iii) where there is systematic monitoring of a publicly accessible area on a large scale.¹⁶

¹² Section 9-13-61-302(2) UCPA and Section 4-715D.4 ICDPA (emphasis added).

¹³ Section 7150(a) & (b) of the Draft Risk Assessment Regulations for California Privacy Protection Agency (“California’s Draft Risk Assessment Regulations”).

¹⁴ Article 35(1) GDPR.

¹⁵ Section 7150(b) of California’s Draft Risk Assessment Regulations. Please note that a subsequent paper in this series will examine in more detail requirements related to ADM.

¹⁶ Article 35(3) GDPR.

Other Approach: Scope of Harm in California—California’s Draft Risk Assessment Regulations require a data protection assessment where the processing will present a significant risk to “consumers’ privacy.”¹⁷ Unlike other states, which refer to a risk of harm to consumers generally (and not specifically to their privacy), California’s language appears to limit the scope of harm that will trigger a data protection assessment. However, California’s draft regulations would require organizations to classify the source (or type) of harm to consumers’ privacy as either constitutional, discriminatory, economic, physical, reputational or psychological (see additional discussion in Section C below).¹⁸ Given the expansive range of harms purporting to fall within the ambit of privacy, it is unclear whether the California approach is in fact more limited in scope than the laws in other US states.

Other Approach: Prior Consultation in EU GDPR and Prior Restraints in California, Colorado and New Jersey—The GDPR requires an organization to consult the relevant regulator prior to processing where a data protection impact assessment indicates that the processing would result in a high risk and the organization cannot put in place safeguards that sufficiently reduce the risk.¹⁹ US state privacy laws contain no similar prior consultation requirement or option. Still, the lack of such a requirement or option arguably produces a more restrictive approach, as organizations subject to certain state laws (i.e., California, Colorado and New Jersey) are explicitly prohibited from processing if the assessments conclude that risks to consumers’ privacy outweigh the benefits, in which case they have no further recourse with a regulator.²⁰

FINDINGS & RECOMMENDATIONS:

- In pursuit of a harmonized and unified approach, organizations tend to create a single assessment based on the highest common denominator, currently the GDPR, and supplement it to comply with the US state privacy laws as necessary (e.g., sale of data under the CCPA). While some have successfully employed a single template, the sustainability of this approach is being challenged with the enactment of additional new laws and different regulatory interpretations, which, if the current trajectory of enacting different state laws continues, will only get worse.
- Organizations do not appear to differentiate among the various standards that trigger data protection assessments, namely heightened risk, significant risk and high risk. Instead, they treat them synonymously. This more unified approach has not been tested in enforcement contexts, but it could leave organizations vulnerable if enforcement agencies determine that these risk thresholds should be interpreted differently. Regulators and lawmakers should endeavor to converge around one of these terms or explicitly indicate that they will not treat them as materially different.

¹⁷ Section 7150(a) of California’s Draft Risk Assessment Regulations.

¹⁸ Section 7152(a)(8) of California’s Draft Risk Assessment Regulations. See Section C, Other Approach: Prescriptive Content Requirement in California and Colorado.

¹⁹ Article 36 GDPR.

²⁰ See, for example, Section 7155 of California’s Draft Risk Assessment Regulations, Section 6-1-1309(1) of the CPA and Section 9(a)(9) of the NJCPA.

- Regarding privacy laws in Utah and Iowa (which do not explicitly mention data protection assessments), organizations nevertheless report using the same risk assessment criteria as explicitly set forth in other state laws. This practice furthers uniformity across jurisdictions and ensures the consistent application of privacy measures.
- In cases where state laws lack clear guidance or interpretation on specific issues, organizations turn to GDPR standards for guidance and consistency. However, organizations are paying particular attention to California’s Draft Risk Assessment Regulations, recognizing that their enforcement and application may ultimately deviate in notable ways from the standards and guidelines set by GDPR over the long term.
- Rather than imposing a blanket prohibition on processing when risks of processing outweigh benefits, states should enable organizations to consult with the regulators on mitigations that would allow for processing to move forward. The establishment of such a mechanism is notably more feasible in jurisdictions with a dedicated supervising authority, e.g., California. State regulators should also offer additional guidance, such as Frequently Asked Questions (FAQs), regarding potential risks and suitable mitigation measures and strategies. This would help organizations to reduce the risk associated with processing to a reasonable level and to proceed with processing activities without the need for consultation.

Table 1. What is the trigger for preparing data protection assessment?

WHAT IS THE TRIGGER for preparing data protection assessment?	
Heightened risk of harm	CO CT DE NH FL IN MT NJ OR TN TX VA
Implicit-reasonably foreseeable risk of harm	IA UT
Significant risk to consumers' privacy	CA
High risk to rights and freedoms	EU

Findings and Recommendations
Greater consistency and clarity across and clarity across key definitions will enable organizations building and operating meaningful protections.
Organizations do not tend to differentiate among the standards that trigger data protection assessments.
Standards should be treated as substantially similar.
When risks surpass benefits, organizations should be able to consult regulators for mitigations to enable continued processing.

Source: Centre for Information Policy Leadership

C. The Elements of Data Protection Assessments

Most Common Approach: Weighing Risks and Benefits—Most US state privacy laws (California, Colorado, Connecticut, Delaware, Florida, Indiana, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Virginia) require similar elements in data protection assessments, including asking covered entities to illustrate how their risk assessments weigh the benefits of the processing against the risks that it may cause to individuals, and which safeguards are in place.²¹ In addition, they prescribe similar factors to be considered, including (i) the use of deidentified data, (ii) reasonable expectations of consumers, (iii) the context of the processing and (iv) the relationship between the covered entities and consumer whose personal data will be processed.²² In that regard, the most common approach mirrors the GDPR, which does not prescribe a particular format but requires that an assessment contains, at a minimum, the following: a systematic description of the proposed processing and the purposes of the processing, assessment of the necessity and proportionality of the processing operations, an assessment of the risks to the rights and freedoms of individuals and the measures, safeguards, security measures and mechanisms implemented.²³

Other Approach: Prescriptive Content Requirements in California and Colorado—California and Colorado follow a more prescriptive approach regarding the content of data protection assessments. Although it is possible to argue that the most common approach also implies elements of the more prescriptive approach by asking organizations to balance between the benefits and risks associated with processing activities, California and Colorado require these elements explicitly.²⁴ In addition to the content requirements laid out in the most common approach, they require a data protection assessment to include the following specific considerations:

- (i) a short summary of the processing activity;
- (ii) categories of personal data, including sensitive data;
- (iii) the nature and operational elements of the processing activity, e.g., processing methods and retention periods;
- (iv) the purpose of the processing activity;
- (v) the sources and nature of risks to the rights of consumers (e.g., constitutional, discrimination, economic, privacy, security, physical, reputational, psychological, unfair or deceptive treatment, impairing consumers' control over their personal information, exploiting

²¹ Section 7152(a)(7), (9) & (10) of California's Draft Risk Assessment Regulations, Section 6-1-1309(3) CPA, Section 8(b) CTDPA, Section 12D-108(b) DOPPA, Section 16-501-713(2) of FDBR, Chapter 6-Section 1(c) ICDPA, Section 9(2) MCDPA, Section 507-H:8(II) NHPA, Section 9(b) NJCPA, Section 8(2) OCPA, Section 47-18-3206(b) TIPPA, Section 541-105(b) TDPSA and Section 59-1-576(b) VCDPA.

²² Ibid.

²³ Article 35(7) GDPR.

²⁴ Section 7152(a) of California's Draft Risk Assessment Regulations and Rule 8.04(a) of the CPA Rules. Please note that the CPA Rules implement the CPA, a comprehensive privacy act enacted in 2021. Both CPA and the Rules entered into effect on July 1, 2023.

- consumers’ vulnerabilities in accessing essential goods and services) and safeguards to address those risks;²⁵
- (vi) description of how the benefits outweigh the identified risks, as mitigated by the identified safeguards;
 - (vii) relevant internal actors and external parties contributing to the assessment;
 - (viii) any internal or external audit conducted in relation to the assessment, including the details of the audit process; and
 - (ix) dates the assessment was reviewed and approved.²⁶

Other Approach: Specific Type of Processing Activities—Some states (i.e., California, Colorado and Connecticut) also prescribe additional content requirements for data protection assessments with respect to specific types of processing activities. California would prescribe additional requirements for a business using ADM technology,²⁷ including whether it consulted with external parties in its preparation or review of risk assessments and, if not, why the organization did not do so, and which additional safeguards were implemented to address risks to consumers’ privacy that may arise from the lack of external party consultation.²⁸ In addition, in instances where an organization processes personal information to train AI or ADM technology, California would also require that it provide other persons using the technology an explanation of the appropriate purposes for which they may use the AI or ADM.²⁹ Colorado has additional requirements for businesses processing personal data for profiling purposes,³⁰ e.g., an explanation of the training data and logic used to create the profiling system.³¹ Finally, Connecticut has additional requirements for businesses offering online services, products or features to known minors, such as

²⁵ As noted above, the listing of these specific types of consumer rights suggests that data protection assessments under California law go beyond identifying consumer “privacy” risks.

²⁶ In California’s Draft Risk Assessment Regulations, information identified in (vii), (viii) and (ix) is offered as Option I for the California Privacy Protection Agency (“CPPA”)’s consideration. Another option (Option II) would require the following: (1) the names and titles of the individuals within the business who prepared, contributed to or reviewed the risk assessment, the individuals’ qualifications and the number of hours that these individuals worked on the risk assessment; (2) the names or categories of external parties with whom the business consulted in preparing and reviewing the risk assessment, and the extent of these parties’ involvement; (3) the name and title of the highest-ranking executive with authority to bind the business and who is responsible for oversight of the business’s risk-assessment compliance, and a statement that is signed and dated by the executive that certifies that the executive has reviewed, understands the contents of and approved the risk assessment; and (4) the date(s) that the risk assessment was presented or summarized to the business’s board of directors or governing body, if such board or equivalent body exists. Thus, in adopting either Option I or II, the CPPA may take a more prescriptive approach than Colorado, especially if it requires the inclusion of the information specified in Option II.

²⁷ Section 7153 of California’s Draft Risk Assessment Regulations.

²⁸ *Ibid*, subsection (7).

²⁹ Section 7154(a) of California’s Draft Risk Assessment Regulations.

³⁰ Rule 9.06 of the CPA Rules.

³¹ *Ibid* Rule 9.06 (f)(5).

identifying the categories and purposes of minors’ personal data that online services, products or features process.³²



















FINDINGS & RECOMMENDATIONS

- Organizations seek to harmonize approaches regarding the elements of data protection assessments across US state privacy laws. However, they are also cautious about exporting compliance with requirements prescribed in one jurisdiction to another that does not have similar requirements, particularly if certain aspects are excluded from the scope of a regulation. Indeed, some states require assessments to cover types of data not addressed by other state laws; for instance, California and EU GDPR include employee data, unlike other states, and Connecticut specifically demands additional content elements for processing minors’ data. Organizations are structuring their assessments accordingly. While this strategy is currently manageable for many organizations, it may become more challenging if additional laws with distinct and prescriptive requirements emerge in the future. Such a scenario could force organizations to develop stand-alone assessments for each state, resulting in duplicative processes and inefficient use of resources and time that could instead be devoted to putting in place meaningful privacy protections.
- Some organizations consider Colorado’s data protection assessment approach as a baseline standard among US states because it is limited to consumer data, includes clear categories of activities that trigger an assessment and provides explicit guidance on the content that should be included in the assessment. Other states might look to it as a model when developing their own requirements.
- While some states (e.g., Colorado and California) require organizations to specify the relevant internal and external parties contributing to their data protection assessments, many US state privacy laws do not include such a requirement. In many organizations, the data protection assessment process is overseen by privacy professionals, with the flexibility to engage a diverse array of internal stakeholders (e.g., legal, IT, information security), as well as external parties (e.g., auditing companies or independent researchers/academics), as needed. Regulators and lawmakers should actively encourage such internal stakeholders and external parties consultation as a best practice. Additionally, there should be incentives in place for effective stakeholder input in risk assessments, such as using it as a mitigating factor in enforcement proceedings.³³

³² Section 10 of the CTDPA Amendments (i.e., An Act Concerning Online Privacy, Data and Safety Protections—Connecticut Online Privacy Law).

³³ Please also see CIPL, *Organizational Accountability in Data Protection Enforcement: How Regulators Consider Accountability in Their Enforcement Decisions*, published on October 6, 2021, available [here](#).

Table 2. What must be included in a data protection assessment?

WHAT MUST BE INCLUDED in a data protection assessment?	
Nothing mandated; factors considered	            
Prescriptive content to be included	 
Additional requirements for certain types of processing	  

Findings and Recommendations

Organizations need flexibility when preparing data protection assessments.

Compliance challenges may arise if additional laws with distinct and prescriptive requirements emerge in the future.

Regulators and lawmakers should encourage internal stakeholder and external party consultation as a best practice.

Source: Centre for Information Policy Leadership

D. Reporting Requirement for Data Protection Assessments

Most Common Approach: Disclosure Upon Request—All states that have an explicit requirement to complete and maintain internal data protection assessments (California, Colorado, Connecticut, Delaware, Florida, Indiana, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Virginia) also require covered entities to disclose their data protection assessments relevant to civil investigations and compliance evaluations to attorneys general upon request (in California, also to the CPPA).³⁴ Data protection assessments are confidential and exempt from public inspection and copying under Freedom of Information Acts.³⁵ Except in California, where the draft risk assessment regulation is silent on this issue, state privacy laws specify that the disclosure of a data protection assessment to the attorney general does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.³⁶

Other Approach: Additional Submission Obligation in California—Unlike other US state privacy laws, California’s draft regulations would require organizations to submit annually to the CPPA the following two documents: the business’s risk assessments in an abridged form and a certification by a designated

³⁴ Section 7158 of California’s Draft Risk Assessment Regulations, Section 6-1-1309(4) CPA and Rule 8.06 of the CPA Rules, Section 8(c) CTDPA, Section 12D-108(c) DOPPA, Section 16-501-713(3) of FDBR, Chapter 6-Section 2 ICDPA, Section 9(3) MCDPA, Section 507-H:8(III) NHPA, Section 9(b) NJCPA, Section 8(3) OCPA, Section 47-18-3206(c) TIPA, Section 541-105(c)&(d) TDPSA and Section 59-1-576(c) VCDPA.

³⁵ *Ibid*, except Section 7158 of California’s Draft Risk Assessment Regulations is silent on the confidentiality of risk assessments.

³⁶ *Ibid*.

executive that the business has complied with the requirements of the data protection assessment article.³⁷

FINDINGS & RECOMMENDATIONS:

- Organizational accountability and a robust risk-assessment regime require organizations to establish processes for conducting risk assessments and maintaining full and up to date records.. Regulators, when concerned about a regulated entity’s processing operations, should and do have access to comprehensive risk assessments as well as summary or abridged forms of them. Privacy laws should require organizations to keep written records of their assessments and be able to make them available in the event of an investigation or enforcement action instead of requiring annual submissions of summary assessments.
- Privacy laws and regulators should clarify that data protection assessments (and summaries thereof, if required) that were prepared in good faith and in compliance with applicable requirements, as well as being able to produce such data protection assessments or summaries on request, can serve as a mitigating factor in an enforcement context. Such a regulatory approach will serve as an incentive for organizations to provide comprehensive and accurate risk assessments (and/or summaries, where required).
- In a jurisdiction requiring the submission of a summary or abridged form of risk assessments, organizations should only be required to submit summaries for processing activities that meet a certain risk threshold and then again in the event of any material changes to the processing, which could include changes in business models, risk, law, technology and other external and internal factors (see more on review requirement in Section E below). This approach streamlines processes for both organizations and regulators, minimizing unnecessary bureaucracy and workload, and ensures a more efficient system.
- Lawmakers or regulators should provide the specific elements to be included in the summary and an online template that organizations can use to submit their risk assessment summaries. This will give organizations notice regarding what is expected in the summary and help ensure consistent responses and ease of review by regulators. Clear regulatory guidance is also essential to proactively prevent potential future allegations of misrepresentation or inappropriate discrepancies between the summaries and the comprehensive risk assessments, especially in the event of a request during an enforcement action.

³⁷ Section 7158 of California’s Draft Risk Assessment Regulations.

Table 3. When must organizations disclose a data protection assessment?

WHEN MUST ORGANIZATIONS DISCLOSE a data protection assessment?	
Upon request by civil authority	CA CO CT DE FL IN MT NH NJ OR TN TX VA
Mandatory submission of abridged version	CA

Findings and Recommendations

- Making data protection assessments available to civil authorities upon request should be sufficient.
- Disclosure should not constitute a waiver of attorney-client privilege or work product protection.
- Mandatory filings expose organizations to greater risk.
- Regulatory guidance is crucial to preempt potential misrepresentations or discrepancies between summaries and comprehensive risk assessments.

Source: Centre for Information Policy Leadership

E. Review Requirements for Data Protection Assessments

Most Common Approach: States Silent on Reassessments—The majority of states (Delaware, Florida, Indiana, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Virginia) do not specify any requirement regarding how often organizations should review and update data protection assessments.

Other Approach: Reassessment in California and Colorado—On the other hand, California and Colorado prescribe that organizations should review and update the data protection assessment as often as necessary and appropriate, and in particular if there is any material change to the processing operations that are the subject of such data protection assessment, e.g., changes in negative impacts to consumers’ privacy associated with the processing, including the sources of these negative impacts.³⁸ This is similar to the EU GDPR approach where the controller is required to carry out a review of data protection impact assessments at least when there is a change of the risk represented by processing operations.³⁹

Other Approach: Minors in Connecticut—Connecticut only prescribes a review requirement in the context of processing activities regarding minors: organizations shall review data protection assessments as necessary to account for any material change to the processing operations of online services, products or features, where they have actual knowledge, or willfully disregard such knowledge, that their consumers are minors.⁴⁰

³⁸ Section 7156(b) of California’s Draft Risk Assessment Regulations and Rule 8.05(b)&(d) of the CPA Rules.

³⁹ Article 35(11) GDPR.

⁴⁰ Section 10(b)(1) of the CTDPA Amendments. In addition, Connecticut only prescribes a retention requirement in the context of processing activities regarding minors. It specifies that organizations that offer an online service, product or feature to consumers—where they have actual knowledge, or willfully disregard such knowledge, that

Other Approach: Reviewing Period for ADM in California—The California draft risk assessment rules provide an option for the CPPA to consider whether to incorporate one of the following obligations into the final regulation: risk assessments for processing that uses ADM technology shall be reviewed and updated at least (i) annually, (ii) biannually or (iii) once every three years.⁴¹

Other Approach: Reviewing Period for Profiling in Colorado—In Colorado, data protection assessments that address processing for profiling in furtherance of decisions that produce legal or similarly significant effects for a consumer shall be reviewed and updated at least annually and include an updated evaluation for fairness and disparate impact and the results of any such evaluation.⁴²

FINDINGS & RECOMMENDATIONS:

- Different statutes have different requirements for review and revision of data protection assessments, with regulations in some jurisdictions proposing reviews at regularly recurring intervals for specific activities, such as automated decision-making. Organizations indicate that differences in review requirements will have important implications for their privacy programs and program implementation/operations as they seek to ensure compliance with applicable statutes. CIPL recommends an approach that requires review when there has been a material change in the way data is processed and used, such as a change in technology, use of data, purpose of processing, processing practices or applicable laws.
- A review may also be necessary when there are changes in the organizational or societal context surrounding a processing activity, such as the identification of new groups vulnerable to discrimination. Conversely, regulators and lawmakers should recognize that certain changes could lower the risk as well. For example, a processing operation could evolve so that decisions are no longer automated, or profiling processing may not constitute a legal or similarly significant effect anymore; thus, the review may conclude that the organization is no longer required to conduct and maintain a data protection assessment.

these consumers are minors—must maintain documentation concerning data protection assessments for at least three years, or as long as they continue to offer those services, products or features. See Section 10(b)(2)(a) of the CTDPA Amendments.

⁴¹ Options for the CPPA’s consideration for Section 7156(a)(2) of California’s Draft Risk Assessment Regulations.

⁴² Rule 8.05(c) of the CPA Rules.

Table 4. When must an organization review a data protection assessment?

WHEN MUST AN ORGANIZATION REVIEW a data protection assessment?	
No review period specified	CT DE FL IN MT NH NJ OR TN TX VA
Review as necessary and appropriate, and if there is any material change	EU CA CO
Additional review requirements for certain types of processing	CA CO CT

Findings and Recommendations

There is no consensus among organizations on how long to review data protection assessments.

Review should be conducted when there has been a material change in the way data is processed and used.

Source: Centre for Information Policy Leadership

F. Mutual Recognition of Data Protection Assessments

Most Common Approach: States Support Mutual Recognition—All states that have an explicit data protection assessment requirement (California, Colorado, Connecticut, Delaware, Florida, Indiana, Montana, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Virginia) and the EU GDPR recognize that a single data protection assessment may address a comparable set of processing operations that include similar activities.⁴³ In addition, all of these except California and New Jersey recognize that if a covered entities conducts a data protection assessment to comply with another applicable law or regulation, that data protection assessment is deemed to satisfy the requirements of the law in question if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted under the law.⁴⁴

Other Approach: Different Recognition Threshold in California—In California, there is a higher threshold to achieve recognition of data protection assessments conducted in compliance with the requirements of

⁴³ Section 7157(a) of California’s Draft Risk Assessment Regulations, Section 6-1-1309(5) CPA, Section 8(d) CTDPA, Section 12D-108(d) DOPPA, Section 16-501-713(4) of FDBR, Chapter 6-Section 1(d) ICDPA, Section 9(4) MCDPA, Section 507-H:8(IV) NHPA, Section 9(d) NJCPA, Section 8(1)(c) OCPA, Section 47-18-3206(d) TIPA, Section 541-105(e) TDPSA,; Section 59-1-576(d) VCDPA and Article 35(1) GDPR.

⁴⁴ Rule 8.02(b) of the CPA Rules, Section 8(e) CTDPA, Section 12D-108(e) DOPPA, Section 16-501-713(5) of FDBR, Chapter 6-Section 1(e) ICDPA, Section 9(5) MCDPA, Section 507-H:8(V) NHPA, Section 8(4) OCPA, Section 47-18-3206(e) TIPA, Section 541-105(f) TDPSA, Section 59-1-576(e) VCDPA and GDPR. Please note that the New Jersey Comprehensive Privacy Act does not address the mutual recognition of data protection assessments. However, there is potential for clarification in the future, as the Act grants rulemaking authority to the Director of the Division of Consumer Affairs in the Department of Law and Public Safety. This authority allows the Director to promulgate rules and regulations deemed necessary to fulfill the objectives of the Act. See Section 15 NJCPA.

another jurisdiction. In California, a business is not required to conduct a duplicative risk assessment if the business has conducted and documented a risk assessment for the purpose of complying with another law or regulation that meets all the risk assessment requirements prescribed in California.⁴⁵ The draft regulation would also require that a business explain in an addendum to the risk assessment conducted and documented for compliance with another law how it meets all of the requirements set forth in California (the CPPA has not yet decided whether to make the addendum mandatory or optional).⁴⁶

Other Approach: Codes of Conduct—The EU GDPR explicitly takes into account organizations’ efforts to comply with approved codes of conduct when assessing the impact of the processing operations, in particular for the purposes of a data protection impact assessment.⁴⁷ While most of the US state privacy laws remain silent on this matter, Tennessee provides affirmative defense to a cause of action for a violation if the covered entities or processor complies with the National Institute of Standards and Technology (“NIST”) privacy framework, or is certified pursuant to the APEC Cross-Border Privacy Rules (“CBPR”) system (available for a covered entities) and Privacy Recognition for Processors system (“PRP”) (available for a processor).⁴⁸

FINDINGS & RECOMMENDATIONS

- Organizations typically perform gap analyses to determine whether their data protection assessments are comparable or if there are gaps that need to be addressed. Regulators and lawmakers can benefit from promoting and acknowledging such gap analysis practices, as they ensure that organizations are proactive in identifying and rectifying potential vulnerabilities. This fosters a robust framework for compliance, ultimately mitigating risks associated with data processing activities.
- Flexible mutual recognition provisions can enable organizations to focus on building strong data protection assessment frameworks that satisfy requirements under multiple jurisdictions. State laws should deem assessments to satisfy data protection assessment requirements if the assessments are reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted. Many US state laws already contain such provisions.
- States can incentivize adoption of good privacy practices by recognizing the value of organizations adopting nationally and globally recognized risk assessment frameworks. More states should follow the lead of Tennessee, which provides affirmative defense to a cause of action for a violation if a party adopts the NIST Privacy Framework, or is certified to the APEC CBPR or PRP systems.

⁴⁵ Section 7157(b) of California’s Draft Risk Assessment Regulations.

⁴⁶ Section 7157(b) of California’s Draft Risk Assessment Regulations leaves in brackets whether the language will stipulate that businesses “shall” or “may” provide the addendum.

⁴⁷ Article 35(8) GDPR.

⁴⁸ Section 47-18-3213 & Section 47-18-3214 TIPA. Please also note that the APEC CBPR and PRP are currently being globalized by the Global CBPR Forum: see Global Cross-Border Privacy Rules (CBPR) [Framework](#) (2023).

- Ultimately, more uniform data protection assessment requirements across the states will reduce the need for such interoperability measures.

Table 5. How can mutual recognition be established for a data protection assessment?

HOW CAN MUTUAL RECOGNITION BE ESTABLISHED for a data protection assessment?	
Reasonably similar in scope and effect	CO CT DE NH FL IN MT NJ OR TN TX VA
Meets all the risk assessment requirements	CA
No mutual recognition specified	EU NJ
Codes of conduct & Certifications	EU TN

Findings and Recommendations	
Organizations conduct gap analyses to assess and improve data protection assessments.	
Flexible mutual recognition enable organizations to focus on building strong data protection assessment frameworks.	
States can encourage privacy practices by recognizing organizations adopting recognized risk assessment frameworks.	
More uniform data protection assessment requirements across states will reduce the need for interoperability measures.	

Source: Centre for Information Policy Leadership