Kilpatrick

Insights: Alerts

FAQs on PIAs: Understanding U.S. State Privacy Impact Assessment Requirements

November 14, 2023

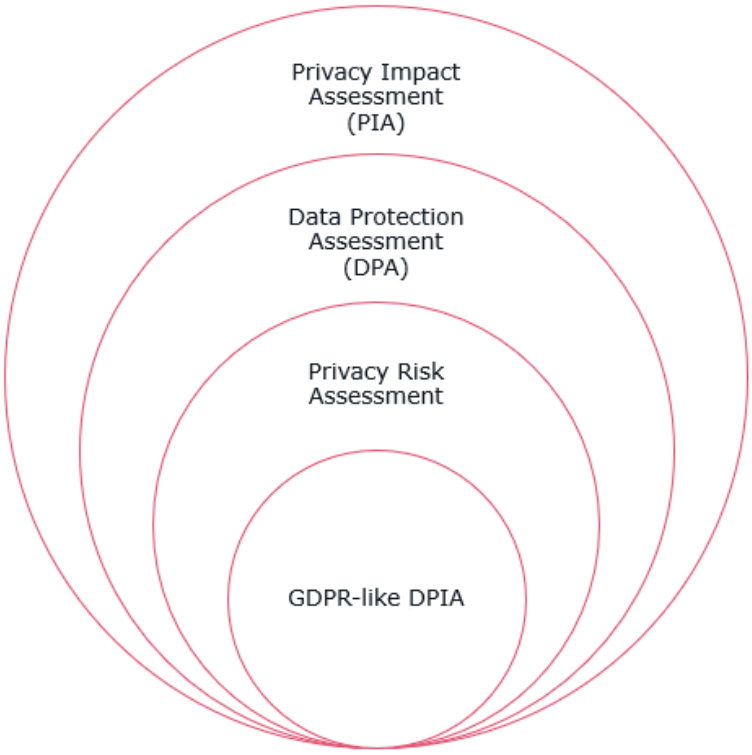
Written by **Meghan K. Farmer**

Privacy impact assessments (PIAs) and/or data protection impact assessments (DPIAs) have formed the practical basis for evaluating initiatives involving personal data in order to comply with various legal requirements for some time, but many companies with a U.S.-only presence have not been subject to a mandatory PIA obligation, per se. Notable exceptions include U.S. federal government agencies, which have had a PIA requirement under the eGovernment Act of 2002, and public sector companies subject to the General Data Protection Regulation (GDPR). However, as new state privacy laws come into effect, U.S. and global companies will need to make sure they have a PIA/DPIA process in place that meets U.S. state requirements, particularly those set out in the California and Colorado privacy laws.

While the PIA requirements may seem daunting, this article answers some commonly asked questions and sets out practical suggestions for aligning an organization's PIA process to the states with the most nuanced laws and achieving a baseline founded on the consistency among the numerous other states with emerging privacy laws.

What is the difference between a PIA, DPA, privacy risk assessment and DPIA?

A PIA is a broad term used to denote a means and process for evaluating projects (processes, solutions, products, apps, etc.) involving personal data. A DPIA is a specific requirement under Art. 35 GDPR for high-risk processing activities, such as large-scale processing of sensitive data. In practice, PIAs are often used to perform an initial assessment of a project and identify the need for further assessment based on jurisdictional impact, type of data being handled, type of processing, and so on, as well as to identify the need for a GDPR "DPIA." A GDPR DPIA requires organizations to evaluate specific characteristics and risks based on EU/UK rights and principles. To add to the complexity, some U.S. state laws now require the equivalent of "DPIAs" though most use the term data protection assessments (DPAs). U.S. state DPAs resemble GDPR DPIAs to some extent but should not be confused with them. It is easier to think of these DPIAs and DPAs as falling within the broader category of PIAs. We refer to PIAs generally as PIAs in order to avoid confusion with other privacy-related acronyms.



Which U.S. States Have Enacted Privacy Laws Containing A PIA Requirement?

The states with comprehensive privacy laws currently on the books containing explicit PIA requirements (as of the date of publication of this article) are Virginia, California, Connecticut, Colorado, Montana, Tennessee, Indiana, Texas, Florida, Oregon, and Delaware. Utah and Iowa currently have comprehensive privacy laws that do not include PIA requirements. Note that other types of laws may contain impact assessment-type requirements, such as NYC's Local Law 144. Note as well that a number of other states have proposed comprehensive privacy laws, including several in committee at the time of publication.

How are the PIA Requirements Structured?

Although there are numerous states with PIA requirements, it is helpful to understand that there is a common baseline structure that is seen across many of the laws. By complying with this baseline, you will be well on your way to a PIA program that addresses state law requirements.

U.S. State Law Baseline: PIAs are generally required before processing personal data in a manner that presents a heightened risk of harm to consumers.

Which States Follow the Baseline Model?

The states that currently follow this “baseline” model (as of October 2023) are:

- Virginia
- Connecticut
- Colorado
- Montana

- Tennessee
- Indiana
- Texas
- Florida
- Oregon
- Delaware

What constitutes a heightened risk of harm to consumers?

Many states (i.e., CT, CO, MT, OR, DE) present the same four examples of situations where heightened risk is present and PIAs are required:

    - Targeted advertising
    - Sale
    - Profiling
    - Processing sensitive personal data

- Others (i.e., VA, TN, IN, TX, FL) present a list of five situations where PIAs are required: the same four PIA triggers listed, and "heightened risk" presented as the fifth, catch-all category.
- Takeaway: Whether "heightened risk" is presented as a non-exclusive list of examples or as a catch-all category of its own, the effect should be the same in practice.

Are there States with Exceptions to the Baseline Requirements?

The regulations and rules for Colorado and California describe PIAs in far greater detail than the wording of most of the statutes. The rules outline the content and scope of the assessment, a list of potential specific harms stemming from processing, and provide helpful examples in a number of cases. Highlights include:

Colorado: Colorado follows the baseline model except that it defines profiling differently than other states by excluding "reputational" harm from the profiling calculus. As noted above, the Colorado Regulations generally spell out more of the considerations that should be made in conducting the assessment, although some amounts to reminders about other obligations under the law, such as considerations of basic privacy principles included as duties of the controller. Similar to the GDPR, the scope of PIA should be proportionate to the scope of risk presented, the size of the Controller, amount and sensitivity of Personal Data Processed, Personal Data Processing activities subject to the assessment, and complexity of safeguards applied.

The Colorado Regulations include a list of what should be addressed (at a minimum) in the PIA. There are currently 13 discrete issues to address, several of which have several subsidiary considerations. The broad buckets include:

- **Description:** Various means of describing the processing activity: **summary**, **categories of data**, **context** (e.g., relationship and c**onsumer expectations**), nature, "organizational **elements**," core **purposes**.
- **Risk/benefit analysis**: Sources and nature of **risks** (of which there is an extensive list of possibilities), **safeguards** to mitigate risks, and a description of how the **benefits outweigh** the risks. The Regulations include a list of modifications that might change the risk level of a given project, including algorithmic

result. CO explicitly requires the organization to review its duties as a controller as part of the mitigation, including transparency, purpose specification, data minimization, avoiding secondary use, care, unlawful discrimination, and with respect to sensitive data. Mitigating factors might include contracts, policies, and procedures.
- **Logistics**: The parties (internal and external) involved in the PIA, audits related to the PIA, dates of review/approval, information about the reviewers, and signatures of the reviewers/approvers.

Two specific scenarios are also contemplated:

- Profiling: If profiling is involved, the controller has to address the requirements of Rule 9.06, which contains specific provisions for PIAs related to profiling activities. This includes a more detailed risk calculus and a significant level of detail explaining the profiling system, which appears to be geared towards automated decision making and AI.
- Sensitive data: If (permissible) sensitive data processing is involved, the controller must detail its process for making sure any related inferences are not transferred and are deleted within 24 hours.

California: As noted, the Draft Risk Assessment Regulations currently require risk assessments for sell/share and sensitive personal data, but a number of other activities are under consideration, potentially making the requirement quite broad. It does not appear to have a catch-all category currently, however. The CA Regulations provide various examples of processing that would require a PIA. Much like CO, the CA Regulations include a list of what should be included at a minimum. There are currently 10 issues to address, also with subsidiary considerations, some of which are still up for Board debate. The issues closely track the CO Regulation buckets, with the similarities highlighted in bold above.

Like CO, the CA Regulations include a lengthy list of potential harms.

- **Description**: Very similar to CO; see above.
- Risk/**benefit** analysis: Very similar to CO. However, although the effect is the same, unlike CO, the CA Regulations require the risk/benefit analysis to explain whether the negative impacts outweigh the benefits (rather than vice versa).
- **Logistics**: The CA Regulations provide two options for the level of information to be included regarding the parties involved in the assessment, with a significantly higher commitment at the executive level in one of the options.

California's Draft Risk Assessment Regulations require risk assessments where an activity presents a significant risk to consumers' privacy, which currently includes selling or sharing personal data and processing sensitive personal data. There are a number of other types of activities that are under consideration for inclusion in the final regulations, such as minors' personal data, using automated decision-making technology (ADMT), employee monitoring, monitoring people in public places (“places that are open to or serve the public”), and using personal data to train AI or ADMT. Should these items make it into the final regulations, the result will be a longer list of enumerated PIA triggers, but it is likely that many of those items would fall within the baseline model catch-all category of “heightened risk.”

The CO Regulations and CA Regulations also explicitly state that stakeholders from across the organization should be involved.

Other States: A few states also have specific thresholds for when PIAs are required, i.e., only organizations that process the personal data of a certain number of individuals are required to carry out PIAs (e.g., Delaware's PIA requirement kicks in for controllers that process/control at least 100,000 individuals' personal data). However, this is largely the exception at this point.

Should PIAs be completed for activities that were already in place before the law(s) went into effect?

Most states do not mandate retroactively applicable PIAs, requiring assessments only for activities that commence after the effective date of the law – but there are a few notable exceptions, such as Florida (retroactive to July 2023), and some that are currently silent on retroactivity, such as California's draft regulations.

Can PIAs that were Completed as Part of Another Compliance Initiative Be Leveraged to Meet State Law Requirements?

Fortunately,, several states explicitly allow for PIAs that were completed for the purpose of complying with other laws to fulfill the PIA requirement for that state, as long as the assessment is reasonably comparable to what is required in terms of scope and effect. (See, e.g., The Texas Data Privacy and Security Act, Sec. 541.105(f)). Those currently include the states following the “baseline model” (i.e., VA, CT, CO, MT, TN, IN, TX, FL, OR, DE). This should apply to PIAs that were completed to comply with non-US laws as well, as long as the scope and effect are reasonably similar, for example, PIAs (not just DPIAs) for GDPR.

The “baseline model” states also allow for one PIA to cover similar types of processing activities Colorado describes this further as a similar set of processing operations/activities with similar types of harm; for example, a toy store chain that collects children's personal data to send birthday coupons and annual coupons. The same PIA can be used to assess both the birthday and annual mailings, across all stores, because it collects the same categories of data in the same way for the similar purposes. (See Rule 8.02).

In addition, most states require organizations to consider similar factors in conducting the assessment, which at its essence is a risk/benefit analysis. Factors for consideration include:

- **Identifying risk/benefits**: Organizations are supposed to “identify and weigh” the direct or indirect **benefits** of the processing activity to the organization, consumers, other stakeholders, and the public against the potential **risks** to the consumer's rights – a calculus that at the outset appears to already favor the benefits given the various groups to which those might apply. CO explicitly requires the organization to demonstrate the benefits outweigh the risks. It also includes a list of at least 11 types of harms that might apply, which range from discrimination to financial injury to psychological harms. CA has a similar structure.
- **Safeguards** that might **mitigate** those risks
- **De-identification** of personal data
- **Reasonable consumer expectations**
- **Context** of the processing
- **Relationship** between the organization and the data subjects

Is a Separate Assessment Required for AI?

Although most of the state privacy laws do not mention AI specifically, AI may be implicated under any number of the processing activities in which PIAs are required. One likely suspect is various types of **profiling**; targeted advertising may utilize AI as well. Watch out for the "heightened risk of harm" catch-all category, which would be especially critical where AI is used to make significant decisions about individuals. In states where employees fall under the definition of "consumer" or "data subject" this will be crucial in terms of evaluating recruits and employees. NYC's Local Law 144 addresses such tools directly, and it appears the (draft) CA Regulations will include extensive requirements for assessing AI and automated decision making technology (ADMT).

The FTC is also taking a strong interest in AI, specifically bias in AI, and especially with respect to the processing/sharing of sensitive data (minors, health data, etc.). Having a documented assessment of how AI works and how the company has controlled for things like bias and hallucinations could be important in the event of a regulatory investigation. The FTC recently issued demands to companies such as OpenAI to gather details for their investigation, and has scrutinized other types of companies as well. See KTS's overviews of legislative and regulatory action at the U.S. federal level here and here.

Organizations might consider adding questions to their risk/impact assessments such as:

- Will the AI system process personal data of customers, employees, third parties, others?
- Are there risks related to (1) discrimination, (2) bias, or (3) unfair treatment stemming from the AI system?
- How likely are these risks to occur?
- What is their potential impact on data subjects (severity)?
- How is the AI system tested for the above risks?
- How does the AI system evaluate and ensure data accuracy?
- How does the AI system prevent errors or outcomes that could harm data subjects?
- What procedures are in place to allow individuals to exercise privacy rights under applicable law? • How will the AI system's performance, risks, and compliance be regularly monitored, evaluated, and updated?

The above is only a sampling of potential questions and should not be considered an exhaustive list. KTS is available to assist in evaluating use cases and developing tailored risk assessments.

Do PIAs Need to be Made Publicly Available?

Generally, state Attorneys General may request the disclosure of PIAs via civil investigative demand (CID) relevant to their investigation but may be exempt from disclosure under U.S. state open records acts.

What are Key Global Considerations?

Note that even where PIAs are not required per se, privacy impact assessments of some variety are widely regarded as a foundational step to complying with a range of other data protection/privacy and security requirements, including implementing reasonable security measures, data mapping/inventory and maintaining records of processing (in support of data subject rights and request fulfillment), and accountability, oversight, and governance obligations. Understanding what the organization is doing with personal data – and having a means to review and approve such processing, is critical to any privacy and security program.

The state statutes also generally provide that the PIAs will be confidential and exempt from disclosure under applicable state freedom of information acts or open records acts, and the usual privileges are not to be waived

as a result (work product, attorney-client). However, this is not necessarily the case under GDPR or other global laws, although other types of protections may apply. For PIAs with implications for company confidentiality, one potential solution is to create a summary version that excludes company confidential information and can be publicly consumed.

Related People



Meghan K. Farmer

t 404.541.6816

mfarmer@ktslaw.com