November 14, 2023

U.S. State Privacy Impact Assessment (PIA/DPIA) Requirements

by Meghan K. Farmer

With the passage of numerous comprehensive state laws, many U.S. companies are now subject to a formal requirement to complete a Privacy Impact Assessment ("PIA"). While the various state and international PIA requirements may seem daunting, it is possible to align an organization's PIA process to the most nuanced laws and achieve a baseline founded on the consistency across the states.

Below are the core concepts that you should be familiar with. See Kilpatrick Townsend's recent Legal Alert for the answers to some commonly asked questions and practical suggestions for approaching the PIA requirements landscape.

Core Concepts/Key Information At a Glance

- Many states follow a "baseline" model which provides that PIAs are generally required before processing personal data in a manner that presents a heightened risk of harm to consumers.
- "PIA" is a broad term for privacy evaluations that also covers more targeted assessments, such as GDPR or GDPR-style data protection impact assessments (DPIAs). U.S. state laws often refer to PIAs as data protection assessments. PIAs are a means of documenting details around personal data use cases / processing activities and are essentially risk/benefit analyses.
- Heightened risk of harm generally includes (but is not limited to) activities involving targeted advertising, profiling, sale of personal data, and handling sensitive personal data.
- Colorado has documented a set of detailed PIA requirements via regulation, and California is expected to finalize a set of detailed requirements for privacy risk assessments very soon.
- For U.S. based companies, model the overall PIA process on the "baseline states". Focus on the common factors triggering PIAs. Layer on CA and CO specific requirements where applicable. If the company plans to expand globally, be sure to include questions about the jurisdictions in which they will be operating.
- Identify additional likely candidates for "high-risk" / "heightened risk" processing based on what the organization does (e.g., the company's business model, data handling, industry, etc.).
- If the company also has GDPR or other global exposure and an established GDPR PIA/DPIA template in place, build in screening questions to see if additional assessments/questions are needed for the U.S. states.
- Include or be prepared to include questions related to AI / ADMT.
- Continue to monitor for developments in the U.S. state privacy arena, as well as municipal-level or topic-specific requirements.

<