REDCLOVER ADVISORS

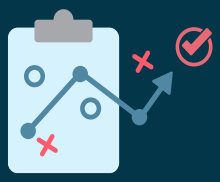
Privacy Risk Assessments PIA/DPIA: Business Guide

www.redcloveradvisors.com | info@redcloveradvisors.com

REDCLOVER ADVISORS

PRIVACY RISK ASSESSMENTS

The Privacy Review Process



All organizations have a responsibility to recognize and assess the risks associated with their personal information processing activities. This likely includes a legal obligation to conduct privacy impact assessments (PIAs), data privacy assessments (DPAs), or data protection impact assessments (DPIAs), depending on the jurisdictions in which the organization operates.

These privacy reviews help organizations identify potential privacy risks so they can implement appropriate safeguards to protect the personal data they process.

1

Privacy Threshold Assessment

A privacy threshold assessment (PTA) is the initial and highest-level review. This determines whether an initiative necessitates a higher-level privacy review like a PIA/DPA or DPIA. The criteria for a PTA can vary, ranging from a simple check to see whether personal information is impacted to more nuanced considerations specific to your operations. A PTA can also help prioritize conducting privacy assessments for existing initiatives.

2

Privacy Impact Assessment / Data Privacy Assessment

A PIA or DPA will then further identify the privacy risks of an initiative involving personal information. In some cases, PIAs/DPAs are required by law. So, make sure you know the rules for the jurisdictions impacted by the initiative.

3

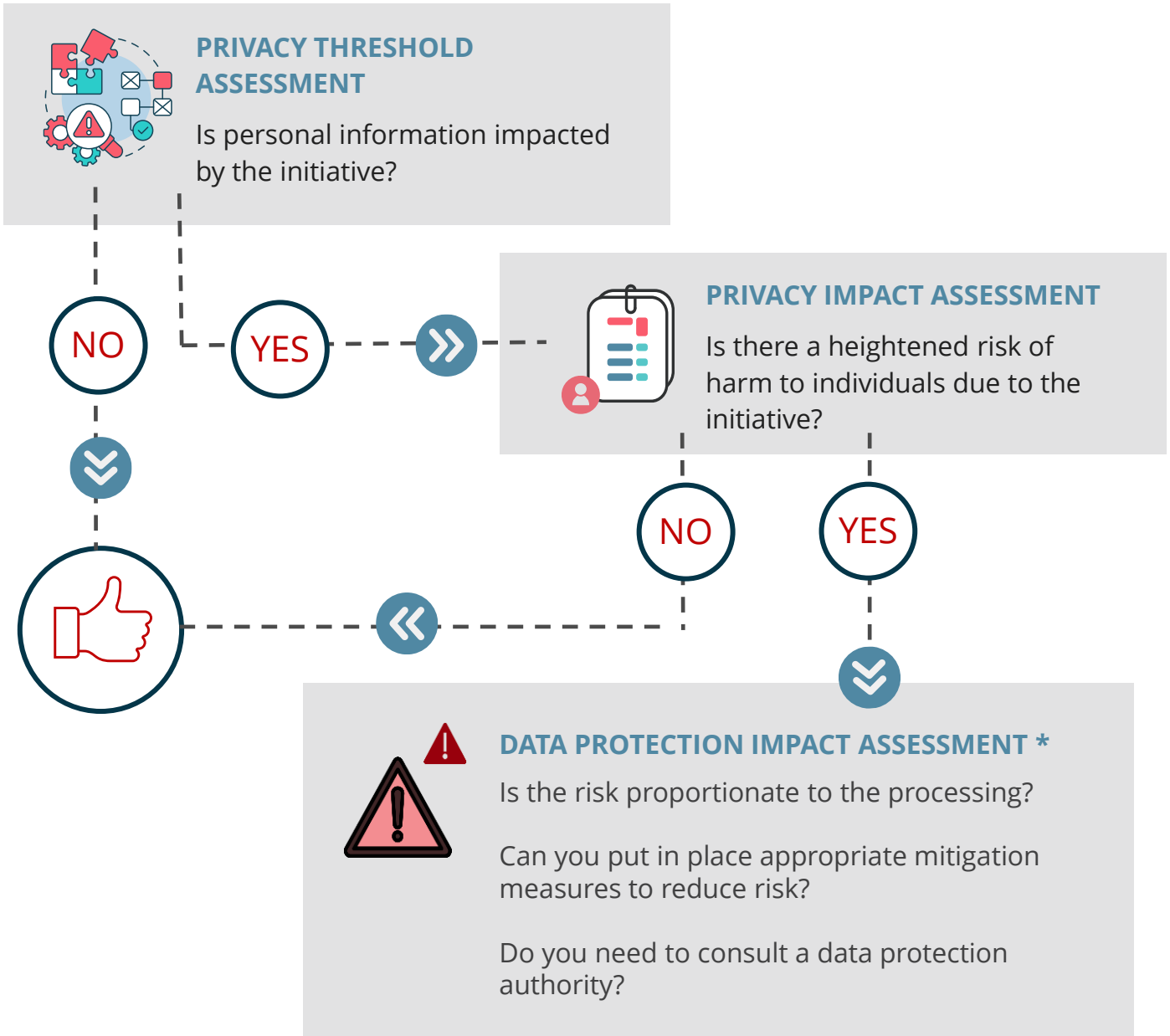
Data Protection Impact Assessment

In some regions, DPIAs are required for certain processing activities. These assessments require organizations to include specific information in the assessment and there are obligations around consulting data protection officers, regulators, and rules around next steps when significant risks are identified.

A Tiered Approach to Risk Assessment

The privacy review process is tiered and how extensive it is depends on your legal obligations and the risk of harm to individuals that you uncover along the way.

Ideally, organizations conduct privacy reviews in the planning phase of an initiative. This streamlines the development and helps ensure that privacy is considered throughout the lifecycle of the initiative. It also helps avoid having to redo elements of the project where privacy hasn't been taken into consideration, saving time and money.



- Data protection laws indicate specific circumstance where companies are required to conduct a DPIA and what information must be included.

Important Considerations

1 THE TYPE OF PROCESSING

Certain types of processing represent greater risk to the rights and freedoms of individuals, and the privacy review process aims to surface those risks. You may also be required to conduct a PIA/DPA or DPIA for certain types of processing. Pay particular attention to initiatives that involve:

- Selling or sharing personal information
- Processing for the purpose of targeted advertising
- Profiling that results in significant legal or similar impact on the individual
- Using new technologies (such as AI)

2 THE CATEGORIES OF PERSONAL DATA IMPACTED

Certain categories of personal data are more sensitive and need greater protections than other categories due to the risk they represent to individuals. Prior to processing these categories of personal data, you may be required to conduct a PIA/DPA or DPIA. Be especially diligent when initiatives involve the processing of sensitive personal information., including but not limited to:

- Race or ethnicity
- Sexuality or sexual orientation
- Religious or political views
- Genetic or biometric information used to identify an individual
- Health information
- Financial information
- Immigration or citizenship status

3 THE CATEGORIES OF INDIVIDUALS IMPACTED

Some individuals are at higher risk of discrimination, fraud or other harms than others, so it's important to take into consideration the individuals likely to visit your website, use your services, or otherwise interact with your organization. Privacy reviews will help you uncover the categories of individuals impacted so you can determine the appropriate processing activities and protections for the dataset.

4 THE JURISDICTIONS IMPACTED

Your legal obligations around privacy reviews are tied to the jurisdictions impacted by a specific processing initiative. Many privacy and data protection laws are extraterritorial, so look at where the individuals are located when determining jurisdiction - not just where you are conducting the processing.

PRIVACY RISK ASSESSMENTS

Set Yourself Up for Success

Privacy Review Questionnaires

Create and implement standard questionnaires for each phase of the review process (PTA, PIA/DPA and DPIA). This ensures that your privacy review process will be consistent across all areas of the business and enables privacy teams to push the work out to business units. Make sure questionnaires come with clear instructions as to how to complete them.

Prioritize Assessments

If you're just starting your privacy review program, you are likely processing personal information in ways for which you haven't assessed risk. Make sure you assess existing practices as well as new ones and use a threshold assessment to determine high-level risks. Then start the privacy review process starting with highest risk first.

STREAMLINE

Work with business units that are heavy users of personal data (e.g., marketing, sales, customer service) to insert privacy assessments into their existing processes.

Teams are more likely to implement privacy reviews if they are involved in the design and you insert as little disruption as possible into existing workflows.

DOCUMENT & MEASURE

Make sure you maintain documentation of all your privacy reviews. You may need to show them to a regulator upon request.

This documentation helps you measure the effect your privacy reviews are having on your organization. Create a metrics program that you can learn from, drives change and shows the value of your privacy program.

EVOLVE

Privacy and data protection laws change, business practices change, and those things impact your privacy risks.

Make sure your privacy review process includes regularly revisiting assessments to ensure they are still accurate and continue to align with your company's risk profile.