Your Checklist For DPIAs

Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs) are required under the GDPR and have become common requirements for several other comprehensive data privacy laws in the last few years. DPIAs are risk assessment audits that help organizations identify, analyze, and minimize the risks associated with handling personal information. DPIAs are typically required for processing data that poses a high risk to someone's rights and freedoms—especially in relation to sensitive personal information—or for "large-scale processing of personal data." Within the GDPR, however, "high risk" and "large scale" are not clearly defined, so it's critical to conduct a DPIA for any major project that requires processing personal data. Here are a few things to keep in mind as you conduct a DPIA:

WHAT TO INCLUDE IN A DPIA

- [ ] **Whose Data You're Processing**
  For example, are you processing the data of patients at a hospital, consumers who purchased your product in the last couple of years, students at several schools across the country, or other categories of data subjects? Different data subjects are protected by different regulations—make sure you know which are relevant.

- [ ] **What Kind of Personal Information You Will Use**
  This will help determine if the PI is sensitive personal information or otherwise. Are you collecting biometric data or the status of someone's race or sexual orientation? Or are you mostly collecting data that you could find in a phone book? Make sure you know what your governing regulations' definitions for sensitive personal information are.

- [ ] **Description of the Processing**
  What is the nature, scope, and context of the processing?

- [ ] **How You Will Use the Data**
  What is the purpose for which you are collecting and processing data?

- [ ] **Description of the Risk**
  Identify and assess the risk to individuals.

- [ ] **Definition of How You Will Minimize That Risk**
  Break down any measures you will take to minimize and prevent risk to the individuals involved.

FACTORS TO ASSESS

- [ ] **Is It Necessary?**
  Is personal data processing necessary and proportionate to meet your goals?

- [ ] **Are the Risks Worth It?**
  Are the risks involved with processing this data worth the desired outcomes?

AFTER THE DPIA AND BEFORE PROCESSING

- [ ] **Determine If There Is Still a High Risk**
  Assess if there is still a high risk to individuals after mitigation and weigh the severity of any impact on individuals.

- [ ] **Do You Need to Contact a Supervising Authority?**
  Under the GDPR, you'll need to do this if the identified risks cannot be sufficiently mitigated.

- [ ] **Publish the DPIA**
  While this isn't required, making a DPIA public can help foster trust with your audience and authorities. Make sure to redact any sensitive information.

- [ ] **Create Your Project Plan**
  Integrate the results of the DPIA into that plan.

- [ ] **Track and Monitor**
  Track and monitor the project against the DPIA to maintain privacy.