Data Protection & Privacy Impact Assessments Done Right

Author : Cat

Date : June 18, 2019

Before embarking on any kind of compliance it is important to understand what the requirements are and when you need to implement them. The GDPR (Global Data Protection Regulation) in the EU states that you have to run a DPIA (Data Protection Impact Assessment) if you are using any data that is highly sensitive or could be high risk if breached. In Canada, with PIPEDA (Personal Information Protection & Electronic Documentation Act), they request a PIA (Privacy Impact Analysis) for all government business, including third parties that work with government.

The *Privacy and Data Protection Impact Assessment* is a risk management tool intended to examine a business' processes, systems, and workflow that handle a user's personal data. The goal is to ensure that both a user's data and their rights are protected to mitigate risk of harm. Companies who fail to run a DPIA in GDPR could see fines as high as 2% of the organization's annual revenue or up to 10 million euro, whichever is greater.

Running the assessment shows due dilligence in privacy but also gives the company peace of mind in having protected data properly. You can include as much or as little in your own documentation. Below is the list of the seven sections we include in our own DPIA template that you may chose to include in yours:

Executive Summary

The DPIA can be a lengthy and technical document. It is helpful to target an executive summary at those unfamiliar with the project. It should include a basic overview of the project, a summary of the areas of privacy and security protection that were assessed, and an overview of the outstanding corrective actions.

Systems & Services

This is the opportunity to describe your product or service. Create a *System Map* (in words or images) which details how the system collects, stores, and analyses data. You can also include technical details about programming languages and storage systems.

Data: Sources, Classifications, and PII

To best understand Personal Data, create a *Data Map* detailing the types of PI (Personal Information) collected and the source. You can then determine if the PI is in fact PII (Personally Identifiable Data). Include the legal basis for the collection of the PII.

Consent

Document what mechanisms you use to gather consent (opt-in by default, opt-in on sign in, opt-out, etc). Include a link to your company's Privacy Policy.

Security

Evaluate the methods you have put in place to secure data in storage and in transfer. Include elements such as encryption and methods to authorize access. This include both physical and digital elements of security.

Retention and Deletion

Discuss what the company policy for retaining data and deleting data upon completion of use or on user request.

Further Actions

List any outstanding actions and recommendations that the company should perform in order to bring their privacy and security practices up to standard.

Be sure to complete your document by having all Privacy stakeholders sign off on the analysis and recommendations.

If you have any questions about Impact Assessments or anything related to Data Privacy Global Compliance, reach out **and we will be happy to help.**