GDPR: DATA PROTECTION IMPACT ASSESSMENTS

Category: Infrastructure and Telecommunications,Media and OTT,Privacy Law, Infosec, and POPIA,Technology Law
written by Sasha Beharilal | May 23, 2018

While there are many similarities between the Protection of Personal Information Act 4 of 2013 ("**POPIA**") and the General Data Protection Regulations, ("**GDPR**") there are also many differences. One of these differences is the obligation that GDPR places on organisations to conduct a Data Protection Impact Assessment ("**DPIA**").

What is a Data Protection Impact Assessment?

This is a process that allows you to identify possible data protection risks to a project. For example, you are a recruiter and your current project requires you to submit 500 curriculum vitaes to your client. The potential data protection risk is that you may not have consent to share curriculum vitaes. In this regard, you will need to acquire consent to mitigate your risk.

If your organisation is thinking about procuring new AI technology to process and store personal information, are there any risks to where the information is stored or how decisions will be made based on personal information? DPIA can assist when making expensive procurement decisions.

In the event that a data protection risk cannot be mitigated, it must be communicated to the Information Commission Office ("**ICO**").

What is included in a Data Protection Impact Assessment?

In essence, the DPIA must describe the nature, scope, context and purposes of the processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks.[1]

GDPR has the potential to have a crippling effect on grossly negligent organisations, for this reason, it is imperative to undertake a DPIA before commencing with a project that involves the processing of personal information. Should there be a breach of sensitive information during the course of a project, and you had not undertaken a DPIA which would have identified the sore points in your project, this could result in the ICO finding you grossly negligent.

With gross negligence comes fines, imprisonment and damaging reputational harm.

What are the steps to take?

Training is absolutely important. Before the start of any project, make it policy to commence the project with a DPIA. The importance of this must be communicated to every individual in the project management process. Once risks have been identified, active measures must be taken to mitigate these risks. Sounds overwhelming, doesn't it? It does not have to. Data Protection and Privacy lawyers will guide you through this process.

[1] Data Protection Impact Assessments
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/