Client Alert: Data Protection Impact Assessment

Date : September 17, 2018

Data Protection Impact Assessments (DPIAs) are one of the key elements of GDPR. They help organisations assess risk and deal with it in a proportionate way. The DPIA process is not new – the UK Data Protection Authority issued their first guidance on Privacy Impact Assessments in 2007, but DPIAs get statutory footing under GDPR and are mandatory in some cases. There is more information on DPIAs in GDPR Navigator, including a film explaining the DPIA process with tips from some of the work that we have done already in this area.

At the end of August the EDPB published a short guide to DPIAs. That follows earlier regulatory guidance. In October 2017 the Article 29 Working Party (WP29) published guidelines on the DPIA process. We summarised that guidance here http://www.corderycompliance.com/client-alert-new-dpia-guidance-issued/. These guidelines were endorsed by the EDPB in Endorsement 1/2018 on 25 May 2018. Some DPAs have also issued their own guidance following the WP29 guidance – for example the ICO's guidance in the UK is summarised here http://www.corderycompliance.com/client-alert-uk-data-protection-regulator-publishes-new-guidance-on-data-protection-impact-assessments/. There's an explanation of the role of the EDPB and the historical role of WP29 in our data protection glossary here www.bit.ly/gdprwords

When should a DPIA be carried out?

It is usually best to start the DPIA process at the start of a project. If you do that you are more likely to be able to put remedial measures in place to deal with risk more easily and more cost-effectively. If you need to consult with a regulator that process can take 4-5 months – this might be another reason for starting early.

EDPB reminds us in the August note that:

"DPIAs must be carried out prior to any processing taking place and every time a new form of processing takes place or the processing is significantly updated. The process should be started as early as possible and undertaken as part of the design of the processing operation, even if some of the processing operations are still unknown. Carrying out a DPIA is a continual process, not a one-time exercise."

An earlier draft of the WP29 guidance suggested that existing processes should be reviewed by 24 May 2021, i.e. within three years of the coming into force of GDPR. The final draft of the WP29 guidance does not include the three year rule, although some DPAs, including the Data Protection Commission in Ireland, have suggested that it may still apply the three year rule.

DPIAs as a mitigating or aggravating factor

DPIAs are important not only because they reduce risk, but also because proper engagement with a DPIA process is likely to be a mitigating or aggregating factor in any penalty. As the EDPB note says:

"However, whatever its form, a DPIA must be a genuine assessment of risks, made by the controller and, in doing so, allow him or her to take the necessary measures to address them. This will result in greater trust and confidence of data subjects, which could in turn result in greater competitive advantage. On the other hand, an incomplete or poorly conducted DPIA could be a factor in a later sanction decision, or possibly result directly in a sanction imposed."

It is important to remember that a DPA has the power to order a DPIA exercise be completed. The ICO's enforcement action in the Royal Free case with Google DeepMind is an example of that in action pre-GDPR - https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/

Importance of training

From our experience DPIAs are the aspect of GDPR that organisations (and their employees) struggle to get their heads around. With proper training however the process can become second-nature and materially reduce an organisation's risk.

More information

There is more information about this and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

Cordery has helped organisations large and small with DPIA tools, templates and training.

For more information please contact Jonathan Armstrong or André Bywater or who are lawyers with Cordery in London where their focus is on compliance issues.