ICO seeks comments on draft Data Protection Impact Assessment guidance

The ICO has for many years championed the benefits of voluntary Privacy Impact Assessments for new, innovative but potentially high-risk types of processing under the Data Protection Act 1998.

The new General Data Protection Regulation (GDPR), which will apply from 25 May, now formalises this situation by making the use of Data Protection Impact Assessments (DPIAs) a legal requirement in certain circumstances.

But make no mistake, this is not just more red tape or an unnecessary burden being placed on data controllers. DPIAs will be an extremely useful tool allowing organisations to positively demonstrate their compliance with data protection obligations, meeting people's expectations of privacy and helping prevent potential reputational damage.

Even where they are not a legal requirement, they can be a very beneficial process for responsible controllers to incorporate privacy by design and by default principles into their projects. These concepts are at the heart of GDPR compliance.

So what is a DPIA?

Essentially, it's a documenting process which will allow an organisation to systematically describe and analyse its intended processing of personal information, helping to identify and minimise data protection risks at an early stage.

As well as being a key element of a controller's accountability obligations under GDPR, an effective DPIA could have real benefits down the line in ensuring compliance, building external trust and avoiding the possible reputational and financial implications of enforcement action following a breach.

Under the GDPR, controllers will be required to complete a DPIA where their processing is 'likely to result in a high risk to the rights and freedoms of natural persons'.

'Likely' does not mean the risk is certain, but it will be the responsibility of the controller to assess the level of risk of their intended processing by making a reasoned judgement on the likelihood and potential severity of harm.

Our guidance includes examples highlighted in the GDPR and also a further list that the ICO is legally required to develop of the types of processing likely to be high risk – we are also seeking comment on this.

Our draft DPIA guidance builds on our previous PIA code, with further detail on specific GDPR requirements. This includes a DPIA template, although controllers who anticipate doing lots of DPIAs may wish to consider develop their own.

It also gives detail on the circumstances when controllers will be required to consult the ICO prior to the processing if they cannot identify measures to reduce the potential risk identified in their DPIA to an acceptable level.

The ICO is required to provide written advice, when prior consultation is engaged, within eight weeks. This period can be further extended where the processing of personal data is especially complex.

As well as offering advice, the ICO could in some circumstances issue a formal warning to an organisation, or even take formal action to ban the processing altogether.

We are seeking comment on the draft guidance published last week, particularly on whether or not it is clear when a DPIA will be necessary.

In addition, we would also like controllers to tell us whether they consider they may need to submit a DPIA to us for written advice in the 12 months following 25 May 2018.

The consultation is expected to run from 22 March until 13 April 2018. We are also planning an ICO podcast on our DPIA guidance in the next few weeks.

We have also published detailed guidance on the area of legitimate interest as a basis for processing under the GDPR.