5 November 2013

RESPONSE TO THE UK ICO'S CONSULTATION ON CONDUCTING PRIVACY IMPACT ASSESSMENTS CODE OF PRACTICE

BACKGROUND

This response is submitted by the Centre for Information Policy Leadership (the "Centre"). Some members of the Centre have contributed to the response, but nothing it contains should be taken as representing the views of any individual member. Understanding the risks involved in the processing of personal data is vital to the development of new products, services, systems and technologies. The members of the Centre are all businesses, each of which is committed to using personal data responsibly and to implementing privacy and accountability within their corporate governance programmes. It is for this reason that the Centre chose to provide input on the ICO's Consultation on Conducting Privacy Impact Assessments Code of Practice ("the Code)") and to submit this response.

EXECUTIVE SUMMARY

1. The Centre welcomes the ICO's Code and believes it will serve as a valuable resource to organisations which are planning and introducing new systems, products, services and technologies which present privacy risks. We see PIAs – alongside a more risk-based approach to data protection – as an important means of improving effectiveness of data privacy regulation and practices on the ground. As with its Anonymisation Code, the ICO in this Code is demonstrating that it seeks to provide concrete guidance to organisations on challenging data protection issues. This will be widely welcomed, not least in contrast to other regulators who emphasise enforcement rather than constructive guidance to promote good practice. The Centre believes that this Code will provide sensible and practical guidance to organisations on the types of issues they should be considering internally and the methodology for recognising, mitigating and resolving privacy risks.

2. Our response focusses on additional suggestions relating to the criteria for conducting PIAs and the need for further clarity on the practical risks and harms to individuals. We also put forward a suggestion for offering incentives to organisations to conduct PIAs. We believe this is a key element in encouraging accountable organisations to maximise the benefits from activities which raise privacy issues whilst balancing the privacy risks.

RESPONSE

Terminology

3. The Centre supports the clarification of the terminology used in relation to PIAs such as "privacy", "projects", etc. The Centre believes it may be helpful to amend references to a new "project" in the Code to include new systems, products, services and technologies. This would make the concept more familiar to private sector organisations. Further examples of such systems, products, services and technologies could be added to the list provided in Chapter 1. Big data analytics, social networking tools, products which monitor individual's activities, and centralised or global IT systems are some examples which could be included.

Guidance on privacy risks

4. The Centre believes that the ICO has taken the correct approach to introducing PIAs by reference to the privacy risks to individuals in its Code. There needs to be much closer dialogue between the hitherto separate disciplines of Risk Management and Data Protection and the Centre is playing a role here.

5. Chapter 6 of the Code is especially helpful as it assists organisations in identifying the relevant risks. Although this is difficult and largely novel territory, the Centre believes that further guidance on the nature of such risks or harms to individuals is likely to be desirable. Organisations do not always find it easy to recognise, or even articulate, concrete privacy risks to individuals, nor have regulators been active in doing so. The Centre believes that organisations and regulators alike will find it helpful for more consensus to be built around the different types of risk or harm to individuals in the privacy context. For example, a classification could be developed around material harm (e.g., financial damage), moral harm (e.g., reputational, intrusion and other intangible harm) and harm to the democratic and societal values of a free society. The Centre is working on a new project to elaborate the benefits of a more risk based approach and attempt a fuller description of the different types of privacy risk. We expect an initial paper to be circulated in Spring 2014, including, of course to the ICO. In due course, it may be useful to reference these harms in (or alongside) the Code so that organisations can understand how best to adopt a holistic approach to PIAs which takes into account the full range of privacy risks or harms.

6. The Centre believes that the compliance risks and corporate risks may be overstated in the Code. Whilst compliance risks and corporate risks must certainly be considered as part of the PIA process, these will generally be the same for all projects. For example, non-compliance with the Data Protection Act 1998 will always be a compliance risk for all projects. Similarly, corporate risks for all projects will consist of enforcement action, reputational damage and distrust of customers, employees, individuals, etc. We therefore encourage the ICO to state these as general risks which arise in relation to the processing of personal data and to re-cast these as further benefits of conducting PIAs. The Code could also provide granular examples of privacy risks to individuals, perhaps by way of a case study which would allow organisations to determine how risks should be captured.

7. A key message which emerges from the world of Risk Management is that risk can never be eliminated entirely and indeed it can be undesirable or counter-productive to make any such attempt. Risk reduction and mitigation should be acceptable as outcomes in their own right, where appropriate. The Centre would like this message to be spelt out as clearly as possible in the Code.

PIAs as good practice

8. The 2013 research which the ICO commissioned from Trilateral gives good examples of where PIAs have been helpful and spells out the benefits of integration with other risk and project management methodologies. It also stresses the need for streamlining and simplification.

9. The Centre welcomes the ICO's approach to PIAs and, in particular, the acknowledgement of the fact that they are not mandatory under UK data protection law. Whilst developments in Europe on the proposed EU Data Protection Regulation envisage PIAs being mandatory in certain circumstances, the Centre is not convinced that PIAs should be mandatory. There is a danger that a prescriptive, mandatory approach will prove to be bureaucratic, burdensome and ineffective. This will damage the current positive reputation of PIAs and jeopardise their value, making them a bureaucratic exercise and an unwanted administrative burden.

10. Whilst there are numerous benefits of conducting PIAs, not least because they minimise privacy risks and enable organisations to build in privacy safeguards saving time and

money in the future (as explained in the Code), they are not suitable for every system, project, product or service, which involves the processing of personal data. The Centre believes that there should be appropriate criteria or triggers for conducting PIAs, even where PIAs are recommended as a matter of good practice. This would allow for a more targeted, risk based approach to be taken by organisations, enabling privacy risks to be balanced with business needs. Annex 2 of the Code provides a list of PIA "screening questions" which are helpful in enabling organisations to understand the triggers. The Centre believes these triggers should be moved into the main body of the Code and re-shaped to provide a non-exhaustive list of when a PIA is recommended or not recommended. Such a list could take the form of a checklist or flowchart. Whilst this may be a challenging task, the Centre believes this will enable organisations, some of which launch new systems, products and services every day, to prioritise completion of a PIA where necessary. The Centre agrees with the screening questions on the whole and suggests the addition of a question relating to whether the project involves the monitoring of individuals. It may also be useful to separate new projects which are utilising personal data for the first time, from on-going projects which are being upgraded or changed in some way, as the considerations are likely to be different.

Scalability

11. The Centre welcomes the comprehensive nature of the Code which covers the full process of completing a PIA, from start to finish. The Centre particularly appreciates the inclusion of project management techniques which will enable PIAs to fit within an organisation's existing business processes. However, the Centre warns against a 'one size fits all' approach in this context and suggests that the ICO should consider whether the Code (or accompanying guidance) should be configured in various forms according to different types of organisation. For example, there could be more concise guidance for SMEs which are unlikely to require the same level of detail as bigger organisations (although the Centre acknowledges that many of the same considerations will overlap). Similarly, large or multi-national organisations may require further guidance on balancing the risks and benefits of a project in order to match their level of sophistication (and resource) when putting appropriate processes in place.

12. It may also be worth considering whether guidance for PIAs for public sector organisations should be made distinct from guidance for private sector organisations. The Centre believes that in relation to the criteria for conducting PIAs (see paragraph 9 above), separate guidance may be useful for public sector organisations. Indeed, it may be appropriate for PIAs to be mandatory for public sector organisations which often handle more sensitive data than private sector organisations. Similarly, in relation to consultation with stakeholders and publication of a PIA, it may be more useful to treat public sector organisations and private sector organisations separately to take account of their obligations under other legislation (see paragraphs 15 and 16 below).

Offering incentives for PIAs

13. The ICO rightly extolls the benefits of conducting PIAs and states that there are many benefits for organisations which conduct them, including: increased likelihood of satisfying compliance requirements, building consumer trust in an organisation; and financial benefits, as PIAs enable risks to be identified at any early stage in the development of a product or service which reduces the cost of dealing with privacy challenges at a later stage when the costs of resolving such issues will be higher. The Centre believes that further benefits of conducting PIAs should be included, such as the boost to an organisation's reputation of being seen to be taking privacy seriously, or as a competitive differentiator in the marketplace. The Centre believes that emphasising these business orientated benefits will encourage more private sector organisations to adopt PIAs, rather than seeing them as a compliance burden.

14. Finally, the Centre also suggests that the ICO consider offering tangible incentives to organisations to conduct PIAs. One option would be for the ICO to spell out explicitly its readiness to take into account whether an organisation has completed an acceptable PIA when investigating a serious breach of the Data Protection Act 1998 and deciding what, if any, enforcement action, should be taken. Similarly, organisations that conduct PIAs could be deemed to be complying with the balancing test requried as part of the legitimate interest ground for processing – hence, enabling these organisations to rely on the legitimate interest ground more frequently in practice. Finally, there could be a link between PIAs and the proposed seal and certification programmes, enabling organisations which conduct PIAs and which are able to demonstrate their implementation, to be fast tracked through a seal or certification programme. The impact of such incentives, could in the Centre's opinion, dramatically increase the take up of PIAs as well as demonstrate the ICO's proactive and constructive approach to data protection more generally.

Consultation with affected individuals

15. The Code of Practice suggests that as part of the PIA process, both individuals within and outside the organisation, whose privacy interests are affected by the project, should be consulted. Whilst this may be appropriate in the public sector context for large scale and risky processing, in the private sector, it is not a practical course of action (see paragraph 12 above). Business confidentiality and other considerations (time, resource and cost constraints) may limit the number of stakeholders who may provide input as part of the consultation process. This is particularly the case in relation to externally affected individuals with whom it would be challenging to ensure proper engagement. Often, organisations do not have a direct relationship with end-customers so it would be unrealistic to require them to canvas input from such individuals. In addition, given the number of new services, products and systems that are launched by private sector organisations, affected individuals may not wish to provide continuous feedback as part of the PIA process. Even if affected individuals do respond, further thought may need to be given to how to interpret such responses and whether the feedback received is truly representative of all affected individuals. The Centre would therefore welcome further clarification in the Code of Practice.

Publication of PIAs

16. The Centre would point out that whilst it is certainly beneficial for reasons of transparency to publish PIA reports, a good practice requirement to do so would pose significant difficulties for private sector organisations, which need to protect their commercial secrets, intellectual property, information security and other business considerations. Whilst the Centre appreciates the ICO's suggestion of redacting the most sensitive elements of PIA reports, it may not always be the most feasible way to maintain confidentiality. In some circumstances, it will not be appropriate to publish any of the content of the PIA report in a manner that is meaningful. Instead, the Centre recommends that rather than publishing a PIA report, organisations be encouraged to be more transparent (perhaps in their Privacy Policy or FAQs) in explaining how the product or service works and what privacy safeguards have been implemented in order to minimise the risk to individuals. Such information will serve the same purpose as the publication of a PIA report but may also be more convenient and accessible to individuals. The Centre does not rule out the possibility that the publication of PIA reports would be useful in the public sector, not least because of the statutory duty to provide information under the Freedom of Information Act 2000 (see paragraph 12 above).

CONTACTS

17. For any questions and queries regarding this response, please contact Bojana Bellamy, President of the Centre for Information Policy Leadership, by telephone: 02072205703 or by email: bbellamy@hunton.com.