Data Protection Impact Assessments: look before you leap

Stephanie Pritchett, Solicitor and Principal of Pritchetts, explains what would be required to comply with the draft Data Protection Regulation's requirements on mandatory Data Protection Privacy Impact Assessments

As most readers will be aware, the European Commission published its proposed new Data Protection Regulation ('draft Regulation') on 25th January 2012. Once it has been approved by both the European Parliament and the European Council, the draft Regulation will replace the current Data Protection Directive (95/46/EC) and will amount to extensive revision of data protection legislation across the European Union. Whilst approval is not currently expected to happen until 2014, it would be prudent for many organisations to start 'tweaking' their data protection policies and procedures now, in anticipation of both the more extensive compliance responsibilities and the potential new increased fines of up to 2% of annual worldwide turnover, a sizable "stick" in anyone's language.

Introduction of mandatory 'Data Protection Impact Assessments'

Amongst the various new requirements set out in the draft Regulation, Article 33 introduces the need for data controllers and data processors to carry out mandatory 'Data Protection Impact Assessments' ('DPIAs') before carrying out high-risk data processing activities. These assessments are not a new concept — 'privacy impact assessments', as they were previously known, have been around for some time. It is the legal obligation to carry out such assessments in certain circumstances that is the new element.

In the UK, whilst there is no legal requirement to carry out a privacy impact assessment ('PIA') under the current Data Protection Act 1998 ('DPA'), the Cabinet Office has instructed all central government departments and agencies that it is compulsory for them to carry out PIAs when developing any new systems. These PIAs should be carried out in line with the guidance set out in the Information Commissioner's 2009 Privacy Impact Assessment Handbook ('PIA Handbook') (available at www.pdpjournals.com/docs/88002).

However, the Information Commissioner's Office ('ICO') has advised that PIAs should be used more widely by all UK public and private sector organisations. This is consistent with the ICO's published strategy that 'privacy by design' and preventative steps at the early stages of projects are far more effective in minimising data protection risks than 'tacking on' measures as an afterthought.

UK organisations that are already experienced in carrying out PIAs will not be as concerned by the new assessment obligations. However, those organisations are in the minority. The new provisions will most likely require most data controllers and data processors to acquire new skills and experience in order to carry out DPIAs and deal with follow up compliance actions.

Of course, the UK regulator along with other national data protection authorities will need to publish new versions of any guidance to take account of changes introduced by the draft Regulation. As a result of this, even those organisations that are currently well-practised in carrying out PIAs, will need to make changes to their current policies and procedures.

When will we have to carry out Data Protection Impact Assessments?

Under Article 33(1) of the draft Regulation, where data processing operations "present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes", the data controller, or the data processor acting on its behalf, will be required to carry out a DPIA to consider what the impact of the proposed processing operations will be on the protection of personal data.

The circumstances requiring a DPIA to be carried out under Article 33(1) are relatively vague and will require a certain amount of subjective consideration by organisations. However, Article 33(2) sets out some of the circumstances which will definitely be considered to present the requisite risks. As a result, there will be no question about the need to carry out DPIAs where the following processing activities are proposed:

(Continued on page 12)

(Continued from page 11)

- a systematic and extensive evaluation of personal aspects relating to a natural person, or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;

- information on sex life, health, race and ethnic origin, or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for the purpose of taking measures or decisions regarding specific individuals on a large scale;

- monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale, e.g. CCTV systems;

- personal data in large scale filing systems concerning children, genetic data or biometric data;

- any processing operations which data protection authorities ultimately designate as being likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes. Authorities will have this right under Article 34(2)(b) of the draft Regulation provided that they establish and make public a list of any processing operations where a DPIA and/or consultation with the authority will be necessary;

- any processing operations which the European Commission ultimately designates as presenting specific risks to the rights and freedoms of data subjects. The European Commission will have this right under Article 33 (6), subject to certain procedures being followed.

The requirements to carry out DPIAs will be relaxed a little for public bodies or authorities that are carrying out processing activities as a result of a European Union legal obligation. In those situations, relevant national organisations will not be required to carry out DPIAs unless national law requires that it is necessary for them to do so in particular situations (Article 33(5)).

Readers may be interested to note that, during the interservice consultation period, further requirements to carry out DPIAs in routine circumstances where employee data are to be processed were actually removed from the draft Regulation. This removal reduced what could have been a very onerous burden on most employer organisations to a collective sigh of relief from industry.

How will we carry out Data Protection Impact Assessments?

Article 35 of the draft Regulation will require all organisations of more than 250 employees, and all public authorities, to designate a Data Protection Officer ('DPO'). It is likely that one of the key roles of these DPOs will be to carry out DPIAs, as well as any necessary consultation with the relevant regulator.

The key elements of the new obligation to carry out DPIAs will be as follows:

Provision of certain information: The DPIA will need to set out (under Article 33(3)): a general description of the envisaged data processing operations; an assessment of the risks to the rights and freedoms of data subjects; and the measures proposed to address the risks as well as the intended safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the draft Regulation, having taken into account the rights and legitimate interests of data subjects and other persons concerned.

Seeking views of data subjects: Data controllers will be required to seek the views of relevant data subjects (or their representatives) on the impact of the intended new processing, without prejudice to the protection of commercial or public interests or the security of the processing operations (Article 33(4)).

Policies and procedures: Data controllers will need to put in place policies and procedures to ensure workers know how to carry out DPIAs (Article 22).

Delegation to processors in certain circumstances: Data controllers will in some circumstances be allowed to delegate responsibility to data processors under the draft Regulation. This may include both the need to carry out a DPIA or to consult with the data protection authority before starting to process information in riskier ways. This new ability to delegate responsibility will make it very important for data controllers and data processors to set out contractually:

- a clear division of any such responsibilities; and

- appropriate warranties and indemnities to ensure that if a breach does occur as a result of inadequate DPIAs or consultation, it is clear who will accept financial liability and responsibility for the breach.

This contractual division of responsibilities may be particularly important, as it is currently unclear from the draft Regulation which party the relevant data protection authority would pursue by way of monetary penalties and other sanctions when any such non-compliance occurs.

Powers of the European Commission: under Articles 33(6) and (7), the European Commission will be able to specify certain standards, procedures or requirements that will have to be followed by data controllers or data processors carrying out, verifying and/or auditing DPIAs. This includes conditions for scalability, verification and auditability.

It seems likely that we will see more information produced in due course in relation to how organisations will be expected to conduct DPIAs and what they should contain. The draft Regulation states that in producing

these standards, the Commission will have to consider specific measures for micro, small and medium-sized enterprises. It is likely that these requirements may reflect the kind of principles set out in the UK regulator's PIA Handbook, such as principles requiring organisations to explain the circumstances and manner in which full scale or small scale PIAs should be carried out.

Organisations will no doubt be hoping that any additional requirements imposed by the Commission will be drafted proportionately, having taken into account the likely size and resources of particular organisations. This is so particularly given the Commission's estimates that DPIAs can range in cost from €14,000 (approximately £11,415) for a small-scale assessment, €34,500 (approximately £28,131) for a medium-scale assessment, and up to €149,000 (approximately £121,489) for a large-scale assessment.

What happens if the DPIA concludes that there is a high level of data protection risk involved in carrying out intended processing operations?

Interestingly, organisations will be required to consult their national data protection authority in respect of any proposed processing which may be considered to present 'specific risks' following the conclusion of the DPIA (Article 34).

Given the potential new fines of up to 2% of annual worldwide turnover for non-compliance, the fact that Article 33 is very broadly drafted, and with the onward reporting requirement under Article 34, it is likely that many organisations may well choose to carry out DPIAs and self-report to authorities in the hopes that the authority will 'sign-off' on projects following that consultation, thereby minimising risks of sanctions being applied. This approach may be informed by current ICO guidance which encourages voluntary breach reporting, and indicates that reduced monetary penalties will be applied for 'holding one's hands up' in a breach situation.

"However, it remains to be seen whether authorities will have the time or resources to be able to give organisations the comfort they need to continue with riskier processing operations, particularly in the timely fashion which may be needed for urgent projects. This will certainly be the case should authorities become inundated with consultation requests, which there is currently a high risk of in the proposed new regime."

However, it remains to be seen whether authorities will have the time or resources to be able to give organisations the comfort they need to continue with riskier processing operations, particularly in the timely fashion which may be needed for urgent projects. This will certainly be the case should authorities become inundated with consultation requests, of which there is currently a high risk of in the proposed new regime.

Perhaps national authorities will produce guidance about the situations where they are likely to engage in consultation (e.g. where there are more chances of 'serious breach' or damage being caused to individuals).

Are DPIAs a good idea?

The introduction of mandatory DPIAs will force organisations to carry out a greater level of data protection due diligence before undertaking riskier data processing activities. Crucially, this work will only be effective if organisations carry out reasonable risk analysis assessments to ensure 'privacy by design' and where meaningful reports are produced, as opposed to organisations simply completing a bureaucratic box ticking exercise (or sub-contracting this work to data processors without proper consideration).

DPIAs should be used by all organisations designing and upgrading new data processing systems and procedures to help ensure privacy and data protection risks are considered at early stages in projects. This can only minimise the risks of breaches occurring further into project timetables and becoming costlier and more resource intensive to deal with.

It is hoped that organisations will not be mandated to only use DPIAs in situations where 'riskier activities' are being carried out, but that they will instead be encouraged to either use DPIAs (or the national authority's equivalent) for other, perhaps less risky, data processing projects.

The UK experience

The ICO currently sets out in the PIA Handbook that PIAs should be used by all organisations in a wide range of circumstances to assist those organisations with data protection compliance by:

- identifying what processing is being carried out;
- identifying the risks to individuals and the organisation of new data processing activities, particularly on projects with a wide ranging scope or using intrusive technologies, or involving sensitive or high risk information;
- identifying the privacy risks beyond data protection law;

(Continued on page 14)

(Continued from page 13)

- identifying problems that might occur before they actually happen, to avoid (in the ICO's words) "expensive, inadequate 'bolt-on' solutions" when the issue could have been more cheaply and effectively resolved at an earlier stage of the project;
- identifying solutions to those risks and problems;
- preventing loss of public confidence and minimising reputation risk to corporations and public sector bodies if a data breach occurs. In the ICO's words, "experience shows that once an organisation's reputation is damaged and trust is lost, it is then very hard to regain that trust";
- creating a 'privacy friendly culture' in organisations; and
- complying with legal and regulatory requirements, in addition to any relevant best practice guidelines.

The ICO recommends the use of PIAs not just where very large scale or risky processing projects are being carried out, but also in many other smaller scale or day-to-day data processing projects. This is discussed in more detail in the PIA Handbook, which sets out numerous examples of projects for which the ICO believes organisations should consider carrying out, at the very least, a small scale PIA. Some of these examples include the following situations:

- before the replacement of existing personal data IT systems;
- when collecting items of personal data from a new third party source;
- before carrying out revisions to data disclosure or staff communications policies;
- before the application of a new technology to an existing purpose;
- before drafting new customer verification procedures;
- when re-designing data collection web-forms;
- before outsourcing or off-shoring business processes involving personal data;
- before the application of existing personal data to a new purpose;
- before enacting changes to data retention policies; and
- before making amendments to the organisation's privacy policy statement.

These circumstances may not all constitute 'riskier' activities which would require a DPIA under the new rules of the draft Regulation but they may nevertheless be circumstances where a PIA would be helpful and preferable to getting caught out.

(For further information on the ICO's current recommendations on how and when to carry out PIAs, see 'Using Privacy Impact Assessments', published in Volume 10, Issue 6 of *Privacy & Data Protection*.)

Conclusion

We may see a dual system evolve, whereby mandatory DPIAs will need to be carried out in 'riskier' situations, (yet to be fully defined by the European Commission), but where national regulators will still encourage the use of PIAs in other circumstances. It will be interesting to see in the UK whether the government still mandates the use of PIAs by central government departments and agencies.

Whatever the position with PIAs, organisations will undoubtedly have to build more time into project timescales to carry out mandatory DPIAs both in order to ensure privacy compliance and risk mitigation and also to consult national authorities where that becomes necessary. This will certainly create a greater administrative burden as well as adding to the implementation costs of many new projects.

Ultimately the payoff could be substantial: tighter compliance, investor and board confidence, good PR and a lower risk of expensive and damaging regulator intervention. Let's all look a bit more closely before we leap.

Stephanie Pritchett
Pritchetts Law
stephanie@pritchettslaw.com

Stephanie Pritchett is the leader of PDP's training session, 'Data Protection Essential Knowledge — Level 2'.

For details of the training session, visit www.pdptraining.com