DPIAs — in light of everything

Olivia Whitcroft, Principal at OBEP, examines the impact of various developments on DPIA procedures, and offers advice for updating DPIAs in the wake of them. Olivia wrote the chapter on Data Protection Impact Assessments in the latest edition of 'Data Protection — a Practical Guide to EU law' (Oxford University Press, 2020)

A lot has happened during the last year. Covid-19 has made us look at how to build health testing and home-working into everyday routines. The *Schrems II* decision (Case C-311/18) shook up our approach to international data transfers. The UK Information Commissioner's Office ('ICO') published two new statutory Codes — an Age Appropriate Design Code and a Data Sharing Code. Agreement on Brexit was saved to the last minute, so we were not sure about 2021 data transfers until we were eating our Christmas turkey the week before.

These developments have changed the risk profile of many data processing activities, prompting the need to review existing Data Protection Impact Assessments ('DPIAs'), and the procedures for conducting DPIAs. In addition, for UK organisations, the new Codes emphasise circumstances in which a DPIA may be needed, and contain useful tools to assist controllers in assessing risks and finding solutions.

This article considers the impact of these developments, and offers some practical advice on how to review and update DPIA procedures in light of them.

A quick re-cap: what is a DPIA?

A DPIA is an assessment of the potential risks of personal data processing activities prior to the commencement of such activities. Under Article 35(1) UK GDPR, DPIAs are required where activities are likely to result in a high risk to individuals. They are also a useful way to assess risks and compliance for lower risk processing activities.

The UK GDPR itself (mirroring the EU GDPR) contains examples of high risk processing activities, including large-scale use of special category data, and systematic and extensive automated decision-making. The ICO has published a (non-exhaustive) list of activities where a DPIA is required, including the offering of online services to children, matching data from different sources, and some tracking activities.

The UK GDPR requires that a DPIA contains at least the following elements: a description of the processing activities; an assessment of necessity and proportionality; an assessment of the risks; identification of measures to address the risks; consultation with data subjects (where appropriate); and advice from the Data Protection Officer (if one has been appointed). Where there are residual high risks following the DPIA, the ICO must be consulted. DPIAs should be reviewed regularly, including (in accordance with the not-very-clearly-worded Article 35(11) GDPR), where there is a change to the risks involved.

Impact of Brexit

The UK is no longer an EU Member State, and therefore assessments of UK processing activities need to be carried out under UK rules rather than EU rules. Whilst these are currently similar to each other, there is potential now for them to diverge. The ICO also has more freedom to adapt its lists of activities requiring (or not requiring) a DPIA, without the need to submit them to the European Data Protection Board, or to follow the EU consistency mechanism.

The transfer of data to and from the UK, now outside the EU, presents new risks and compliance issues. There is also now the concept of 'legacy' data — personal data about non-UK data subjects which were processed prior to the end of the Brexit transition period. At the time of writing, the UK is likely to obtain an 'adequacy' decision for EU to UK data transfers. However, unless and until the UK has an adequacy decision (and should any adequacy decision be lost), UK organisations must continue to apply the EU GDPR to any ongoing processing of legacy data. DPIAs may now therefore need to distinguish more clearly between UK and EU activities, and identify the associated cross-border transfers. Overseas activities that started before 2021 should be detailed separately. The solutions for addressing risks may be different to those within previous assessments, when the UK was part of the EU.

(Continued on page 6)

(Continued from page 5)

Impact of Schrems II

In July 2020, the Court of Justice of the European Union declared that the EU-US Privacy Shield was invalid. This method of legitimising personal data transfers from the EU to the US was formerly used by many organisations (and it was envisaged that, at the end of the Brexit transition period, certified entities could update their Privacy Shield arrangements to include transfers from the UK).

In addition to invalidating the Shield, the Court's decision emphasised that use of Standard Contractual Clauses ('SCCs') to legitimise international data transfers was not quite as simple as just signing the clauses and ticking the compliance box. For each transfer, organisations are also required to do an assessment of the overall risks, taking into account the legal regime of the country of transfer and the practical risks to data subjects. As has always been the case, the transferor also needs to assess whether it and the recipient can actually comply with the SCCs in practice. Adding to the complexity, SCCs have not been updated for many years, meaning that they do not currently align with the GDPR, nor do they cater for transfers from processor to sub-processor, or from processor to controller. There are some proposed new SCCs, which (if also adopted in the UK) may assist to address these issues in the near future.

Processing activities involving international data transfers are now more likely to be assessed as presenting a high risk for which a DPIA is required. It may also be more problematic in some cases to reduce international data transfer risks to an acceptable level. The only clear solution may be to 'avoid' the risks, by not carrying out the transfer at all (for example by keeping data centres within the UK or the EU).

> ***"DPIAs may now therefore need to distinguish more clearly between UK and EU activities, and identify the associated cross-border transfers. Overseas activities that started before 2021 should be detailed separately. The solutions for addressing risks may be different to those within previous assessments, when the UK was part of the EU."***

ICO Codes of Practice: Age Appropriate Design and Data Sharing

The ICO has been tasked with preparing several Codes of Practice under sections 121 to 128 of the Data Protection Act 2018 ('DPA'). In accordance with section 127 of the DPA, these statutory Codes will be taken into account by the ICO and the courts in determining whether or not an organisation is complying with the law (for relevant processing activities).

The Age Appropriate Design Code provides standards for designing online services likely to be accessed by children. It came into force on 2nd September 2020 with a 12-month transition period, meaning that organisations have until 2nd September 2021 to bring their activities in line with the Code. One of the overarching standards of the Code relates to DPIAs. It requires a DPIA to be carried out to assess and mitigate the risks to children who may access a relevant service. Of itself, this is not new: as stated above, the ICO's list of activities for which a DPIA is required includes where online services are offered to children. The Code also provides additional guidance and a new template for conducting a DPIA in this context.

The Data Sharing Code of Practice was submitted to the Secretary of State on 17th December 2020, and it now needs to be approved by Parliament before coming into force. It is a guide for organisations about how to share data with other controllers or joint controllers. It recommends carrying out a DPIA, even if the proposed data sharing activity does not necessitate a DPIA under the GDPR (because there is no specific indicator of a likely high risk).

The Codes also contain new standards and recommendations which should be incorporated into the design of relevant projects and activities, and their guidance may assist with identifying risks and solutions as part of a DPIA.

Impact of Covid-19

DPIA deliberations would be incomplete without considering the changes that have been caused by the pandemic. New processing activities, for instance the testing and monitoring of staff, may require a DPIA before they can be carried out. Existing processing activities may also have been adapted, for example due to the shift to working from home, which changes the location and manner of data processing. DPIAs covering these activities may need to be reviewed on that basis.

The ICO has a Data Protection and Coronavirus information hub, which contains useful guidance for identifying and assessing risks as part of a DPIA. The issues it covers include testing, surveillance, contact tracing, vaccinations and working from home. The guidance emphasises the need to assess whether a DPIA is required, and recommends DPIAs as a way to demonstrate accountability.

Practical steps to update DPIAs

Existing DPIAs should be regularly reviewed, and changes to risk profiles may mean reviews need to take place sooner than previously scheduled. Standard DPIA procedures may also need updating to incorporate new or changed areas of risk, or changes to

acceptable solutions.

The developments discussed in this article are likely to be of key significance for such reviews. Organisations should also factor in any additional changes that affect them.

Below are some ideas for reviews and updates for the different stages of the DPIA process.

1. Review initial assessment or screening questions

It is common for organisations to prepare a standard list of questions or criteria to help them to decide whether or not to carry out a DPIA and what the scale of the assessment will be. New questions could be added to determine whether a project involves use of data to protect against Covid-19 (or similar health risks). ICO Codes should be taken into account when making the decision of whether to proceed with a DPIA. Projects spanning the UK and the EU, or involving other cross-border transfers, may now trigger the need for a more in-depth review than would have been undertaken previously.

2. Update information flows and descriptions of processing activities

Descriptions of processing activities should accurately reflect current cross-border transfers, and note that a transfer between the UK and the EU is now a transfer between jurisdictions with different legal regimes. Data about non-UK data subjects collected prior to 2021 may need to be tagged as 'legacy' data. The template in the Age Appropriate Design Code can be used to facilitate descriptions involving children's data. Information flows should be clear on new types of data or processing which have arisen due to protection against Covid or home-working activities.

3. Review procedures for consultation with data subjects

Organisations should consider how to obtain views of children or parents in line with the Age Appropriate Design Code, and how to consult with employees (or their representatives) about new testing or surveillance activities.

4. Update assessments of necessity and proportionality

Organisations need to consider alternatives to processing activities in the context of new risk profiles, which, for cross-border transfers, may include keeping data locally. This stage of a DPIA should now also assess compliance with the principles of the UK GDPR (distinct from the EU GDPR), and with the new ICO Codes.

5. Review previous risk assessments, and the factors used to assess risks

The *Schrems II* decision may assist to guide assessments of international data transfer risks, and ICO Codes may clarify assessments of activities which they cover. Risk assessments may also change due to social and cultural factors. For example, certain activities used to tackle pandemics could become more commonplace over time.

6. Review whether solutions continue to be appropriate and effective

Previous solutions to address specific risks may no longer be valid, such as the EU-US Privacy Shield for transfers to the US, or measures which rely on the UK being within the EU. Other solutions, for instance the use of SCCs for international data transfers, may no longer be sufficient to bring down risks to an acceptable level. New solutions, such as new SCCs (once approved), are likely to present themselves. The ICO Codes may provide guidance on new solutions for use of children's data and data sharing. If, when risks are re-assessed, there are new residual high risks, consultation with the ICO is required before the processing can proceed.

Final thoughts

Risk profiles are continuously evolving. Once DPIAs and DPIA procedures have been updated, it is time to put the next review date in the diary, and watch out for events which may trigger the need for an earlier review.

What changes will we see in the year to come?

Olivia leads the practical training course, 'Conducting Data Protection Impact Assessments', which is available by eLearning. See www.pdptraining.com for further details.

Olivia Whitcroft
OBEP
olivia.whitcroft@obep.uk