Expert comment

Bridget Treacy is a Partner at global law firm, Hunton & Williams — the views expressed are her own

There is a palpable sense of purpose in Brussels as people return from the summer break. The incoming Commission, under the leadership of President Elect Jean-Claude Junker, has set out its priorities, and data protection reform is high on the list. Similarly, there seems to be a renewed sense of purpose within the Council of Ministers to progress the proposed General Data Protection Regulation ('proposed Regulation').

Work on the proposed Regulation has continued apace under the Italian Presidency, and the Council's proposed amendments to Chapter IV (dealing with controller and processor obligations) have just been published. Although many reservations remain within the Council's proposed text, there is also a sense of progress, and renewed focus on the adoption of a risk-based approach — which will be appreciated by the UK, in particular. The last quarter of 2014 promises to be a busy period in the data protection world.

Council's proposals for Chapter IV

The Council of Ministers is still pursuing its 'partial general approach' to reach agreement on the text of the proposed Regulation. Following the conclusion of the Greek Presidency at the end of June 2014, the Italian Presidency has led work on Chapter IV, with the DAPIX committee setting itself the objective of 'sharpening the risk-based approach' in order to reduce the administrative burden and compliance costs inherent in the proposed Regulation.

Risk-based approach

The Council's focus on building a risk-based approach was evident from the initial discussions under the Irish Presidency, and is further in evidence in the draft proposal for Chapter IV, published on 3rd October 2014.

The risk-based approach is closely linked to the accountability principle which already features in the Commission's draft text. Together, the risk based approach and accountability shift the burden to organisations to ensure that their products, services, technologies and information uses are assessed for risks to individuals throughout the whole lifecycle of data processing, and that appropriate measures are implemented to mitigate these risks. Unless justified by a recognised benefit, organisations are responsible for ensuring that processing will not involve a real likelihood of inflicting significant harm. In some situations, the risk assessment may indicate that the processing should not be undertaken at all. In others, appropriate safeguards or constraints will be needed to mitigate the risks.

Accountability

The amendments proposed by the Council to Article 22, in particular, more closely reflect the concept of accountability. Accountability envisages that organisations will comply with legal requirements, but that they have flexibility to determine how to comply, and how to demonstrate compliance. Instead of prescribing detailed requirements for accountability, the Council's amendments to Article 22 use the language of proportionality. The revised wording (reproduced on page 3) permits controllers to have regard to the 'nature, scope, context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals in determining what measures to implement in order to be able to demonstrate compliance with the proposed Regulation (see Article 22(1)).

Data minimisation

One specific issue raised in the general context of Chapter IV is the obligation of data minimisation. The current Directive (95/46/EC) states that personal data must be adequate, relevant and not excessive for the purpose(s) for which they are collected. In the UK, this has been treated as importing a test of proportionality, so that personal data which are reasonably required for a purpose may be processed and retained.

Article 5(c) in the Commission's text requires that personal data shall be 'adequate, relevant and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled

(Continued on page 4)

Articles 22 and 23 of Chapter IV of the latest draft of the European Council's text, 3rd October 2014

Article 22 — Obligations of the controller
(underlined sections denotes 'new' aspects of wording)

1. Taking into account the nature, scope context and purposes of the processing as well as the likelihood and severity of risk for the rights and freedoms of individuals, the controller shall (…) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.
2. (…)
2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
2b. Adherence to approved codes of conduct pursuant to Article 38 or an approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the obligations of the controller.

Member State positions on Article 22:

Belgium, Germany, the Netherlands and the UK, remain unconvinced by the figures provided by the Commission which demonstrated that the reduction of administrative burdens outbalanced any additional burdens flowing from the proposed Regulation.

With regard to 'where proportionate in relation to the processing activities' (in 2a), Hungary Romania and Poland are of the view that the wording allows too much leeway to controllers.

Article 23 — Data protection by design and by default

1. (…) Having regard to available technology and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the likelihood and severity of the risk for rights and freedoms of individuals posed by the processing, the controllers shall implement (…) technical and organisational measures appropriate to the processing activity being carried out and its objectives, [including minimisation and pseudonymisation], in such a way that the processing will meet the requirements of this Regulation and protect the rights of (…) data subjects.

2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are necessary for each specific purpose of the processing are processed; this applies to the amount of (…) data collected, the extent of their processing, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals.

2a. An approved certification mechanism pursuant to Article 39 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2.

3-4 (…)

Member State positions on Article 23:

Germany thought that, in view of Article 5(c) (requires that personal data shall be 'adequate, relevant and limited to the minimum necessary in relation to the purposes for which they are processed…), the principle of data economy and avoidance, as well as anonymisation and pseudonymisation, should be listed as key options for implementation. The Council is going to debate this point in the context of a debate on pseudonymising personal data.

Czech Republic said it would prefer the wording 'not excessive' to 'necessary' (in 2). The Council said that the term may be changed again in the future in the context of the debate on the wording of Article 5(1)(c).

(Continued from page 2)

by processing information that does not involve personal data'. Article 23 (2) in the Commission's text further requires that 'only those personal data are processed which are necessary for each specific purpose of the processing'. These provisions would result in a shift away from the present focus on proportionate data collection, to one in which data may only be collected where explicitly justified. While this may be a more familiar approach in certain continental jurisdictions, it is new to the UK. This represents a material change and would lead to significant increased costs for all UK organisations as they cleanse any excess data and adjust their collection activities to narrow the data sets.

In the latest draft of Chapter IV, the Council has proposed an amendment to Article 5(c) that deletes 'limited to the minimum necessary' and replaces it with 'not excessive'. In addition, Article 23(2) of the Council's text refers to the implementation of measures for ensuring that, by default, one's personal data which are necessary for each specific purpose are processed. These amendments offer organisations a more pragmatic approach, assuming they survive. A transitional provision would also assist, together with provision for the proposed Regulation to have prospective (and not retrospective) effect in relation to relevant personal data. Whether we will see these changes is not yet known.

Mandatory breach reporting

The Council's change of emphasis on data breach should be noted and welcomed. It places individuals, and the likelihood of harm to them, at the heart of the breach reporting obligation. In particular, the likelihood of a 'specific risk' to an individual would be the key threshold for reporting a breach to both the individual and to the supervisory authority. Further, the use of encryption or similar technologies, as well as steps taken by the controller (including after the breach) to reduce the likelihood of harm to individuals, may remove the need for notification to the individual and/or to the supervisory authority. The latter proposal is significant. Data controllers that have managed a data breach will know that steps can sometimes be taken after the event has been discovered, that minimise the risk of harm to individuals. These proposals will all be welcomed, and should reduce the regulatory reporting burden.

Timeline for proposed Regulation

The Council must reach political agreement on the text of the proposed Regulation before it can enter into discussions with the European Parliament. Various dates for the commencement of discussions with the Parliament have been discussed, but the reality is that no particular deadline drives the Council's efforts. While significant progress has been made by the Council, the general expectation is that its position will not be adopted until the second quarter of 2015, so that discussions with the Parliament might start during the Summer of 2015. A two year transition period is expected after the final text is agreed, so this process still has some way to run.

Big Data guidance

In the last Expert Comment, I referred to the Information Commissioner's Office report entitled 'Big Data and Data Protection', which was the first guidance on Big Data offered by a data protection authority. In that report, the ICO emphasised that there is no general exception for Big Data processing, noting that "Big Data' is not a game that is played by different rules'. A similar message has now been delivered by the Article 29 Working Party.

On September 16th 2014, the Article 29 Working Party adopted a Statement on the impact of the development of Big Data on the protection of individuals' personal data. This two-page Statement summarises a number of key messages on how Big Data impacts compliance requirements under EU privacy law. The principal message, which should not come as a surprise, is that Big Data does not impact or change EU data protection compliance requirements.

In the Statement, the Working Party explicitly rejects the notion that the principles of purpose limitation and data minimisation, or the requirements that data must be adequate, relevant and not excessive in relation to their purpose, might have to be reconsidered in light of Big Data.

These principles are challenging in a Big Data context, but the Working Party gave no ground on this. Indeed, indicating a degree of scepticism, the Working Party noted that the real value of Big Data remains to be proven. It also expressed opposition to calls for a 'use model' or a regulatory model primarily focused on the risk of harm to individuals. Instead, while acknowledging the need for innovative thinking on how key Data Protection Principles might apply in the context of Big Data, the Working Party found 'no reason to believe that the EU Data Protection Principles are no longer valid and appropriate for the development of Big Data.' It left open, however, the possibility of 'further improvements to make [the principles] more effective in practice' in the context of Big Data.

On international issues, the Working Party signalled that it understood the compliance challenges caused by the varying legal requirements in different jurisdictions. It noted that international cooperation is needed to provide consistent guidance on operational and compliance questions, as well as on joint enforcement of applicable rules. This acknowledgement and approach is important, not just for the Big Data context. Close working by regulators around the world, and an understanding of global data protection challenges, is more important than ever.

Here's to a busy Autumn!

Bridget Treacy
Hunton & Williams
btreacy@hunton.com