Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bnai.com

International Information for International Business

Volume 12, Number 8 August 2012

The European Commission's Proposal For Data Protection Reform Generating Calls For Revisions

By Renzo Marchini, of Dechert LLP, London.

The dust is beginning to settle on the European Commission's proposal issued in January this year for the reform of data protection legislation. The proposal is to replace the existing Directive 95/46/EC[1] (the "Data Protection Directive") with a directly effective Regulation (the "Proposed Regulation")[2] (*see analysis at WDPR, February 2012, page 4*). The Proposed Regulation will apply to all areas other than law enforcement; a new directive applicable to law enforcement is also in the legislative process.

Since January, respected commentators have been commentating, regulators have been opinioning, and businesses have been lobbying. To bring us up completely to date, EU Member State governments have been making reservations and the European Council has prepared a revision leaked by statewatch.org[3] .

The revision, dated June 22, 2012 (the "Council Revision"), takes into account comments from various Member States on just the first 12 of the 91 articles. The revision also takes into account comments made at meetings of the European Council committee dealing with information exchange and data protection ("DAPIX").

Although by no means comprehensive, a flavour of the strength of feeling aroused by the original Proposed Regulation is clear from this revised version. In its notes to the draft document, the Council makes clear that almost all of the delegates at the DAPIX committee meetings felt that there were too many delegated acts (provisions under which the European Commission is empowered to set more detailed rules). Several thought that a regulation was inappropriate and, indeed, preferred a directive.

Many of the changes deal with what might be called drafting points (complaints that some language is unclear, unnecessary, too vague, and so on), but others highlight significant resistance to points of principle. It is the latter which are addressed in this article.

The fact that the revision is preliminary (amendments stopping at Article 12) means that it is not really possible to see a full picture even in relation to the amendments which have been made, since, for example, there are changes to definitions which may well be linked to changes which might be being suggested in some later articles. For example, the definition of "personal data breach" appears (with other definitions) in Article 4 — and this definition is the subject of much comment. However, the substance of the data breach notification requirement proposal is in Articles 31 and 32 (and so not yet commented on). It is possible to get some sense of the resistance to the initial proposal, but it is inevitable that not all concerns will have been expressed only in relation to this definition. The same point applies to other definitions (and substantive provisions) which appear in the earlier part of the document but interrelate (or depend fully upon) later provisions.

This article, therefore, summarises the most significant changes or requests for change issued by Member States and that appear in the Council Revision. There

have, of course, been other detailed comments on the Proposed Regulation, not least from the UK Information Commissioner's Office (the "ICO") (*see analysis at WDPR, April 2012, page 5*) and from the EU Article 29 Data Protection Working Party (the "Working Party") (*see WDPR, April 2012, page 23*), and this article draws on those commentaries to provide a fuller context.

'Household' Activity Exemption (Article 2.2(d))

An interesting debate is being had in relation to the "household" activity exemption (Article 2.2(d) of the Proposed Regulation). This is the important exemption that states that people using personal data for their own personal use are not subject to data protection law. The exemption already appears in the current Data Protection Directive, and, in that context, issues of interpretation of precisely how it applied reached the courts in the *Lindqvist* case in 2003[4] . The European Court of Justice held that posting personal data about an individual on a website was outside the exemption, since the information would be made available to an indefinite number of people.

This case came before the massive advent of social media networks. Delegates believed that the exemption should be lost when personal data is posted without the protection of privacy settings (so that any member of the public can access it); and the consensus is that that is what the law is and would be on the present drafting. Nonetheless, Belgium would like to make the matter beyond doubt by adding a recital.

Definition of 'Personal Data' (Article 2)

The Proposed Regulation amends the definition of "personal data" in an attempt to make clear that using online identifiers (such as internet protocol addresses and cookies) will bring data processing into the scope of the rules (a question that is heavily debated under the current law).

The capturing of IP addresses and similar online identifiers into the scope of the definition of "personal data" was the subject of an earlier adopted opinion of the Working Party (on the concept of personal data, Working Paper 136). It is not surprising, therefore, that the Working Party (in its opinion on the Proposed Regulation) welcomes this being made express. The ICO in its opinion on the Proposed Regulation agrees. Both bodies, however, criticise the appearance of a recital (number 24 — a late addition to the text) which mitigates against the clarity by saying that it is not "in all circumstances" that such identifiers are personal data. The ICO prefers a formulation which makes clear that, where IP addresses or similar identifiers are processed with the intention of targeting particular content at an individual, or otherwise treating one person differently from another, then the rules are engaged.

It is clear that the language around the online identifiers concept is confused and will likely be cleared up during the legislative process. Given that regulators have long been seeking jurisdiction over this type of online activity (online targeting using cookies/IP addresses), the concept (clarified) will likely remain. And so it is no surprise that the Council Revision accepts the idea of expressly specifying that online identifiers are captured, which is consistent with the tenor of the debate over the last few years.

A second change to this definition relates to the meaning of "identifiable". As with the current Data Protection Directive, data will be captured not only if the data subject is identified but also even if the data subject is only "identifiable". In the Proposed Regulation, this is spelt out to be by "means reasonably likely to be used".

In respect to the issue of identifiablity, the Council Revision wants to apply a test — in answer to commentary (by the United Kingdom, amongst others) — that "means reasonably likely to be used" is too broad; instead, says the proposed new wording, efforts to identify individuals need to be proportionate.

Territorial Scope (Article 3)

The Proposed Regulation widens greatly the scope of EU data protection law. The Data Protection Directive did not readily apply to businesses established outside the European Union (unless they used "equipment" or a service provider within the European Union). The Proposed Regulation would apply to the processing of personal data of EU data subjects even where the relevant data controller is not established in the European Union but where the processing relates to the offering of goods or services to, or the monitoring of, EU residents.

The Working Party appears to welcome the inclusion of non-EU resident data controllers in the scope of the Proposed Regulation in this manner. It does in fact go further, requesting a clarification that "offering goods or services" includes those offered that come at no cost to the data subject. It also feels that the definition of monitoring data subjects (found in the recitals to the Proposed Regulation) should include those cases even where the controller does not actively create a "profile" of the data subject concerned, but merely analyses or predicts the subject's behaviour in some way. In other words, arguing for an even wider jurisdictional test.

The ICO is far more circumspect than the Working Party. Whilst it acknowledges that bringing non-EU data controllers under the EU regime is desirable, the ICO states that it is doubtful of how far this is achievable in practice. The ICO, therefore, states that, in its opinion, the Proposed Regulation should be more open about its limitations with respect to entities outside the European Union.

The Council Revision contains an explanation that the European Commission stated at the DAPIX meetings that this extension of territorial scope is a requirement of human rights law. France, in fact, the Council Revision makes clear, like the Working Party, wants a wider test: Any processing of personal data about EU residents should be covered, not just when goods/services are offered or individuals are monitored. The Czech Republic wants to retain the current "equipment" test. By contrast

   ISSN 1473-3579

to all these positions, the United Kingdom (ever the pragmatist in data protection circles) seems to have disagreed (echoing the earlier ICO view), requesting the removal of the entire paragraph, leaving the only jurisdictional test being that of "establishment". Having said that, as the document makes clear, the Commission is not likely to be swayed by a consideration of whether enforcement is practical; the sense is that the Commission will feel it important to set down a marker to cross-national companies that they are expected to comply with EU rules even if they are not "established" there.

'Consent' (Articles 4 and 7)

Consent is an important concept in data protection law. Consent under the current law (at least in some Member States) may be inferred from circumstances. The Proposed Regulation now requires that consent be "informed" and "explicit", with a "clear affirmative action" or "statement". If a data controller relies on consent, the controller has the burden of proof on showing that it was given. Significantly, consent cannot be used when there is a "significant imbalance" between the data subject and the controller.

The ICO welcomes the stricter test of "explicit" consent being required, but has reservations as to the invalidity of consent where there is a "significant imbalance" between the data subject and the data controller. An example is between an employer and an employee, but the ICO does not accept that that means consent within the workplace cannot be valid. The ICO gives an example of collecting "next of kin" information in case there is an accident — this is not legally required, and so "legal necessity" as an alternative legitimising basis would not be available. Consent here would seem to be genuine and non-controversial despite the imbalance.

By contrast, many delegations at the DAPIX meetings criticised the additional requirements to consent as unrealistic. For example, Ireland queried whether the proposed requirements would lead to "click fatigue"[5]. In reply, the Commission argued that this definition merely clarified the 1995 Data Protection Directive concept of consent, which does not allow for silent or implicit consent, a position (the Council Revision makes clear) with which Ireland disagreed. Further debate is inevitable on this point.

Main Establishment (Article 4)

The Proposed Regulation contains provisions attempting to ensure that data controllers (or processors) operating in more than one jurisdiction should be regulated only by one national authority. The Proposed Regulation proposed to do this by means of reference to an organisation's "main establishment". The regulation defines "main establishment" as, for controllers, the place of the controller's establishment in the European Union "where the main decisions . . . are taken; [or] where the main processing activities . . . take place". For data processors, it is "the place of its central administration in the Union".

The Working Party takes the view that the definition, as currently drafted, does not adequately cover all corporate entities. It states that the overall purpose of knowing where an organisation's "main establishment" is, is to determine the lead data protection authority. However, the current definition makes no allowance for medium or large enterprises that have multiple subsidiaries in different jurisdictions: The actual processing may take place in one Member State, although the "main decisions" take place elsewhere. For data processors, the processing may occur in one jurisdiction, but quite conceivably the "place of its central administration" may lie elsewhere.

The ICO takes a similar view. It argues that multinational corporations take decisions in multiple countries, some of which may be outside the European Union, or that they may even outsource the processing entirely. The definition, as currently drafted, makes no allowance for such eventualities.

Neither the Working Party nor the ICO makes any suggestion as to how to deal with these problems.

The Council Revision does not really address these issues, either. It merely adds an expansion of the definition of main establishment applicable to processors, dealing with the possibility that a processor may not have a "central administration" within the European Union; in that case, it would be considered established where the "main processing activities take place".

Notification of Personal Data Breaches (Articles 31 and 32)

The Proposed Regulation mandates that, in the event of any personal data breach, the controller must notify the relevant supervisory authority without undue delay, and at any rate within 24 hours. There is no express triggering threshold (for example, that the breach be particularly severe or be likely to cause problems for individuals); all breaches are caught. Where the controller does not notify the authority within 24 hours, it must provide a reasoned justification for not doing so. Where the data breach emanates from a processor, it is under an obligation to alert and inform the controller immediately following the breach.

For certain breaches (where there is likely to be an adverse effect on the individual), the data subject should also be notified (but after the regulator is notified).

The Working Party agrees with the introduction of an obligation to notify the controller's supervisory body. However, it cautions that the scope of the duty should be more clearly defined and restricted, to prevent the supervisory bodies being "swamped" with processing notifications of relatively minor breaches.

Interestingly, the Working Party recommends adopting a two-stage process to notifying the supervisory body: to make a first, limited notification within 24 hours of becoming aware of the breach; secondly, for the controller to have an opportunity to make a further notification should it be unable to provide full details within 24 hours.

The ICO also favours the introduction of the notifica-

tion obligation. It agrees with the Working Party that there should be an adequate "trigger" to prevent the supervisory bodies from being "swamped" by inconsequential notifications. The ICO also feels that the 24 hour time limit is unrealistic — and that data controllers will be faced with an unnecessary burden in informing the supervisory body of their "reasoned justification" for their failure to provide information within 24 hours when, the ICO argues, they should be concentrating on rectifying the breach.

The ICO further criticises the current drafting, stating that the obligation currently is for the breaching controller to notify the supervisory body first, before the individual is notified. This is coupled with no obligation on the supervisory body to deal with notifications without undue delay, and the ICO considers that this may lead to notifications building up at the supervisory body, with the individual still unaware that his or her personal data privacy has been breached.

The commentary in the Council Revision makes clear that many Member States are fearful that the present trigger may lead to over-notification (as mentioned above, the comment here is made in the context of the definition of "personal data breach"). Nonetheless, there is no indication of any overriding objections to the possibility of such laws. Denmark, with other Member States concurring, points towards the German law as being a suitable model, namely, notification being required only when there is the possibility of "significant" harm.

Conclusion

This article should give a flavour of the debate that is going on amongst legislators, but it is hard from the limited information available to sense where the debate will end up. Clearly, wherever we end up, there is a long way to go. The Council Revision dealt with just 13 percent of the substantive provisions, and in doing so there were a total of 147 footnotes explaining the changes and summarising Member State views (some of which notes had divergent comments from different countries).

Arguably, the more controversial of the provisions in the Proposed Regulation — such as the right to be forgotten, compliance obligations, data protection officers, cross-border data flows, the real substance of data breach notification, and enforcement, amongst others — appear later. But, even ignoring this point, extrapolating the number of comments thus far to the remainder of the proposal, it is easy to see that the Regulation (if it is to survive at all) is due for a very bumpy ride indeed.

NOTES

[1] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] European Commission Communication No. 11 of 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[3] http://www.statewatch.org/news/2012/jun/eu-council-revised-dp-position-11326-12.pdf.

[4] *Bodil Lindqvist, Case C-101/01 of 6 November 2003.*

[5] As arguably is occurring in relation to cookie consent as a result of the recent changes.

Renzo Marchini is Counsel at Dechert LLP, London, and a member of the World Data Protection Report Editorial Board. He may be contacted at renzo.marchini@dechert.com.

  WDPR ISSN 1473-3579