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 2 February 2012

Cloud Computing Under The European Commission's Proposed Regulation To Revise The EU Data Protection Framework

By Renzo Marchini, of Dechert LLP, London.

The European Commission's recently proposed Regulation to replace the EU Data Protection Directive is designed to "enhance opportunities for companies that want to do business in the EU's internal market, while ensuring a high level of data protection for individuals"[1] (*see analysis in this issue*).

This article explores to what extent the proposed Regulation would impact upon the use of cloud computing in the European Union.

The Current Situation

The new Regulation forms part of the European Commission's overall strategy for the so-called "digital economy", which it unveiled in its 2010 paper, *A Digital Agenda for Europe*[2] . The broad aim, as described by Commission Vice-President and Justice Commissioner Viviane Reding, is to make "the Digital Single Market more accessible for both businesses and consumers"[3] , allowing the European Union to become more competitive, as well as setting the standard for data protection regulation worldwide.

To further this aim, the proposed Regulation has three objectives: to create legal certainty; to simplify the regulatory environment; and to provide clear rules for international data transfers.

Two recent examples in the context of cloud computing provide a timely illustration of the types of problems faced by users of cloud computing which could be resolved by the new Regulation.

Firstly, in February 2011, the Danish Data Protection Agency rejected Odense Municipality's application to use the cloud service "Google Apps" to store data in relation to its public schools (*see analysis at WDPR, April 2011, page 13*). Odense Municipality stated that data would be transferred initially to Google Ireland Limited; Google subsequently informed the Agency that it holds all data in numerous data centres worldwide, including in the United States and Europe. Thus, data would be shared between Denmark and Ireland; then between Ireland and potentially every other country in which Google operates data centres (be it the United States, within the European Economic Area or others).

It is difficult to see how the Regulation would assist the take-up of cloud services within the European Union.

The Agency's view was that any Google data centres in the United States would be covered by the EU-U.S. Safe Harbor Framework; thus Odense Municipality was permitted to store data there as well as in Ireland.

However, the Agency decided it must assume that data

would be transferred not only to Ireland and the United States, but also to all the other countries in which Google maintains data centres, including those neither in the European Economic Area nor the United States (and covered by Safe Harbor). It therefore deemed that Odense Municipality would not comply with current legislation because it was not proposing to enter into a contract based on the European Commission's standard contractual clauses with Google's individual data centres.

A second recent example of current strictures comes from the attitude taken by the Dutch government. In September 2011 it took a hard line against U.S. cloud providers: Government departments were severely restricted in using such providers to process government IT data. The Dutch government's reasoning is that the U.S. Patriot Act requires U.S. companies to provide data to the U.S. authorities if requested under the Act.

Whilst the Commission undoubtedly wants to promote the establishment and operation of cloud servers within the European Economic Area, currently many substantial data centres are located elsewhere. This poses a challenge to the Commission: balancing the Digital Agenda and opening the digital economy to EU businesses with the need to have in place adequate safeguards for data transferred outside the European Union.

The legal issues for EU undertakings (whether public sector or private enterprises) wishing to entrust their data to cloud providers are well known and centre around two main issues: 1) whether it is appropriate for the cloud customer to entrust security of the personal data to a cloud provider; and 2) whether it can do so when the data might be stored outside the European Union.

The question explored here is whether the proposed new Regulation will make these compliance issues easier to navigate.

In addition, the Regulation throws up other issues likely to be relevant to cloud computing: an increased enforcement regime (in particular, fines) and data breach notification.

First a preliminary point of characterisation which becomes relevant.

Roles and Responsibilities of 'Controllers' versus 'Processors'

The EU Data Protection Directive (95/46/EC) (the "Directive") draws a distinction between a "controller" and a "processor" that pervades through all other provisions. Largely, a controller under the Directive has much by way of responsibility, whilst (at least, in most jurisdictions) the processor has no regulatory responsibility (and has only to comply with the contractual obligations with the controller).

The definitions of "controller" and "processor" remain largely the same under the proposed new regime.

As a departure from the current position that processors have no direct regulatory responsibility, under the new Regulation a processor would also have responsibility for security (see Article 30). Moreover, regulators would be able to enforce the provisions of the Regulation (and it seems not only those which are expressly stated to be an obligation of the processor, but also more generally (see Article 52(1)(a) and 53)).

In particular, Article 27 would prevent the processor from processing data except on instruction from the controller or under applicable EU law; Article 28 would require the processor to adequately document its processing; and Article 29 would require the processor to co-operate with any relevant supervisory authority.

At present, many cloud providers would argue that they would be considered to be processors (and thus avoid those obligations placed only on controllers). Nonetheless, following the EU Article 29 Data Protection Working Party's opinion on the SWIFT case[4] and the Working Party's subsequent opinion on these important definitions[5], it is not possible to be absolutely certain that this would be the case in the eyes of regulators and enforcement agencies. The definitions being the same, it is unlikely that the regulators would take a different view of such facts as existed in SWIFT. There will likely remain doubt as to whether a cloud provider is a processor or a controller.

Despite this expansion of regulatory oversight of processors, many cloud providers would still hope that, under the new regime, they would be considered to be processors (and thus avoid even wider regulatory obligations).

Security and Appointing Processors

Article 30 of the Regulation would require both the controller and the processor (in other words, both the cloud customer and the cloud provider) to ensure that there were appropriate security measures in place. Of course, a contract would need to be put in place (Article 26) and this article is substantially the same as the provisions in relation to appointing processors in Article 17 of the Directive, although it is somewhat expanded. Some of these expanded provisions may indeed make it more difficult than the current Directive to use cloud services. For example, the processor could not "enlist another processor" and could be appointed only with the permission of the customers (Article 26(2(d)). This would prevent a software as a service (SaaS) provider, say, from using an infrastructure as a service (IaaS) provider's services without the customer's permission. Clearly, cloud providers will include general language to allow sub-contracting at will — but would that be enough in regulators' eyes to fulfil this requirement?

As is well known, there must be a written contract in place and that contract must oblige the processor to act only on instructions from the customer and require the provider to comply with obligations equivalent to those of the seventh principle. We return to this below, but note here that due diligence into security would be required.

The Regulation proposes the same obligation as appears in the Directive to ensure the controller undertakes appropriate due diligence in relation to the processor.

   ISSN 1473-3579

The Minimum

The Regulation would not change the difficulty currently experienced by the customer having to accept a "standard" security offering from most cloud providers. At a minimum, a contract with a cloud provider would deal with security in the most general of terms, such as, "the provider will use reasonable efforts to keep data secure". More sophisticated customers will (certainly in a traditional outsourcing) wish to set out some level of detail about what in fact will be provided and are having to learn to trust a cloud provider. The economics of the cloud depend on it being a standard offering, perhaps in a multi-tenanted architecture. As such, the provider is not able cost-effectively to tailor its security mechanisms for specific customers.

Other than the dramatic changes in the enforcement regime to be introduced, which may make customers more wary (certainly in the light of the inevitable resistance of U.S. providers being asked to give indemnities for the substantial fines which may be due), nothing in the Regulation seems to affect this problem.

Ongoing Monitoring: Contractual Rights to Audit?

A further requirement of the current regime is the obligation in Article 17(2) imposed upon the controller that it must "ensure compliance with the [security] measures" by the processor. This is often interpreted to require the contractual ability physically to inspect the provider's facilities, and so stated to be hard to fulfil in the context of cloud services. If that is the case, then of course nothing has changed and the cloud has not been liberated. If that is what is required, then in a full "cloud" procurement involving data being located in multi-tenanted virtual servers in unspecified locations (perhaps simultaneously and ever-changing) or simultaneously in multiple locations, it would remain nigh on impossible to acquire cloud services when personal data was involved. However, a better view (to which I subscribe) is perhaps that the obligation does not go that far, and that this aspect of the security obligation might be complied with by other controls, such as a requirement for full monitoring and reporting by the provider itself or to undergo full security certification by an accredited organisation.

Location of the Data and Cross-Border Data Flows

Much of the adverse commentary relating to the ability of EU customers to use cloud services is based on an assessment that the United States (where many cloud providers are located) does not provide an "adequate" level of protection for personal data as required by Article 25 of the Directive.

Some cloud vendors have recognised this restriction and are willing to give the assurance that data will remain in a particular country (perhaps for additional fees). Some of the major IaaS providers, for example, will tell their EU business customers for at least some of their products that data will reside only in EU server farms.

Other providers, salesforce.com, for example, openly state that their data will not remain in the European Union. If this is the case, then one of the various mechanisms to legitimise that transfer under the eighth principle may well need to be put in place.

Position under the Directive

The following options are currently available:

- Keeping data within the European Union or in a country deemed automatically adequate (by means of a Commission decision under Article 25(6) of the Directive). This of course excludes the United States.
- Safe Harbor: A U.S. cloud provider could be on the Safe Harbor list (salesforce.com and Google are).
- Standard clauses: Standard clauses are another solution which generally work well from a customer's point of view, but cloud providers do not like them, as they would have to accept additional liability under the terms.
- "Self-assessment": This is available in the United Kingdom and certain other countries but not generally throughout the European Union. A customer could "self-assess", that is, reach its own view that the personal data once transferred is adequately protected. In many cloud situations, when 1) the data is not particularly sensitive, 2) a sensible security diligence has been undertaken, 3) proper contractual language is in place dealing with security, and 4) the cloud provider is a reputable company of substance, it will not be unreasonable for the customer to satisfy itself that there is adequate protection. Many (certainly, UK-based) cloud customers will have relied on this.
- Other methods: For completeness, it is worth noting that there are other methods for legitimising transfer, although they are unlikely to be helpful for most cloud solutions. Binding Corporate Rules facilitate transfers throughout groups; as such they may be of use in relation to so-called "private clouds" but not otherwise. Consent to the transfer from all relevant data subjects and also where the transfer is necessary to perform a contract with the data subject are also potentially available.

Position under the Proposed Regulation

The Regulation promises harmonisation in particular by being directly applicable. Accordingly, there would be more consistency between various national regulators as to how these rules were applied. However, a downside for those in some countries (such as the United Kingdom) is the lack of flexibility which has to date been shown.

The following options would be available under the Regulation:

- Again, keeping data within the European Union or in a country deemed automatically adequate. The Regulation proposes greater guidance as to how the Commission determines the adequacy of a particular country (Article 41 of the Regulation). Countries

deemed adequate under the present regime would not lose that status (Article 41(8)).

- Safe Harbor would also be adopted under Article 25(6) and so would also continue into the new regime by virtue of Article 41(8).
- Standard clauses would remain as an option. There is no express saving provision providing that those model clauses approved under the old regime could continue to be used; but nonetheless that outcome can be expected.
- Binding Corporate Rules, consent, and necessity for a contract all would remain (see Articles 43 and 44).
- Some form of the "self-assessment" method set out above is expressly discussed, but in a manner which is unlikely to be helpful to cloud adoption. Article 44(1)(h) is worth setting out in full:

  "the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary".

Unlike the approach taken in the United Kingdom (or elsewhere) under the "self-assessment" regime, however, the emphasis here seems to be on an *ad hoc* transfer (not "frequent or massive") as opposed to the continuing outsourcing of data management to a cloud provider. There are also proposed requirements to document the assessment and to inform the regulator of the fact of a transfer. This is unlikely to be at all useful to a potential cloud customer.

Accordingly, not much is proposed in the provisions around data transfer to facilitate cloud take-up in the European Union. Indeed, the main substantive and relevant change is the proposed removal of the ability of a cloud customer to take its own view on the protection of the data. Many data controllers will see this as an opportunity missed.

Data Breach Notification

Article 31 of the new Regulation proposes a general data breach notification requirement[6]. A cloud customer suffering a breach of security of the data (when the data is in the hands of the processor) would be obliged to notify the supervisory body without undue delay. The controller must justify why this has taken more than 24 hours, if this is the case. Of course, when data processing is outsourced (including cloud), prompt breach notification can generally happen only if the provider informs the controller. The new provision duly would oblige the processor (here, the cloud provider) to inform the controller of any personal data breach immediately after it had established that there had been a breach.

However, where the cloud service provider was in fact also a data controller, the obligation to inform the supervisory authority would seem to lie jointly with both parties. Given the relatively complex information requirements prescribed by Article 31(3), there would be the theoretical potential for both parties to inform the supervisory authority independently, with the possibility of conflicting information. It therefore seems that the cloud service contract should specify who would be informing the relevant regulators.

The notification to the supervisory body must contain certain information, including the nature of the breach, recommendations for mitigating the breach, the consequences of the breach, and measures the controller proposes to take to address the breach. The controller must document any breaches (the facts, effects and remedial action taken) sufficiently so that the supervisory authority may verify the controller's compliance with Article 31.

Lastly, as part of the extra-territorial expansion of the proposed Regulation (grabbing the targeted processing of personal data of EU citizens, even by non-EU entities — see Article 3), the obligation to inform the controller would seem to apply also to non-EU-based cloud providers. Thus a U.S. cloud provider would be obliged by the Regulation to inform the customer of a breach. (It is a general criticism of this extra-territorial reach that it may be impossible to enforce against non-EU entities, and that criticism applies equally here.)

Enforcement

Under Article 79 of the Regulation, the relevant supervisory bodies in each EU member state would be given the powers to enforce breaches of the Regulation against controllers and processors. It is important to note that the sanctions in this article would not be fixed: They are to be "effective, proportionate, and persuasive", on a case-by-case basis. The supervisory body would have to take into account the nature, gravity and duration of the breach, *etc.*

In any cloud context, perhaps the biggest issue here is the fact that a failure to comply with the security provisions (Article 30) could lead to a fine of up to 2 percent of the annual global turnover of the person in breach. The same also would apply if the customer did not notify a data breach in contravention of Article 31. Notwithstanding that providers (as processors) may also be liable, given they are directly subject to these articles, a cloud customer of course relies on the provider's security assurances, and on being informed of a data breach, and may be subject to a fine as a result of the provider's failure.

Clearly, bigger customers with negotiating power may well be able to extract appropriate indemnities from a cloud provider in relation to any fine resulting from such failures. However, most customers would be forced to contract on the provider's standard form of contracts. One aspect of cloud computing which is often cited as being different from other technology deals is the take-it-or-leave-it aspect of the technical solution. In keeping with the commercial and technical advantages of the solution being easy to set up, easy to scale, and easy to con-

   ISSN 1473-3579

trol changes, it is also equally easy to contract: A customer simply accepts the provider's terms without question. Customers acquiring a very standard cloud offering would have no scope for negotiating terms.

Where contracts are not negotiated, as a recent study makes clear[7] , many providers accept very little liability at all (if any) for data security breaches and problems.

It remains to be seen whether this increased exposure for a breach (in circumstances where financial liability could not be passed on to a cloud provider (clearly, brand damage will never be passed on)) makes customers more hesitant about trusting their data to the cloud.

Conclusion

It is difficult to see how the Regulation would assist the take-up of cloud services within the European Union. The regulatory difficulty that exists under the present Directive would remain (cross-border data flow issues, restrictions on the appointments of sub-processors, and so on), as would certain conceptual difficulties (whether a provider was a processor or a controller).

Moreover, in some respects the position arguably would be more of a hindrance. For example, there would be an increased regulatory burden upon providers (who are at present not subject to substantive provisions directly): They would be responsible for security, and regulators would be able to enforce the Regulation directly against the processor. There also would be the potential for substantial fines.

In short, the Regulation would solve neither of the two problems currently experienced by EU customers and the service providers seeking to sell to them. In the long term, it may encourage EU customers to use EU service providers, but given the predominance of the United States in this sector, it would do little in the short term to "liberate the cloud". In this respect, it could be seen as a missed opportunity.

Of course, there is some way to go before the Regulation hits the statute book, and business is already commencing an intensive lobbying process.

NOTES

[1] Viviane Reding, Speech/12/26, available at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=HTML&aged=0&language=EN&guiLanguage=en.

[2] Commission communication COM (2010) 245, available at: http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf.

[3] Speech/12/26, available at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=HTML&aged=0&language=EN&guiLanguage=en.

[4] EU Article 29 Data Protection Working Party Opinion 10/2006 of November 22, 2006, on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP 128), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf.

[5] EU Article 29 Data Protection Working Party Opinion 1/2010 on the concepts of "controller" and "processor", WP 169 of February 16, 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

[6] There is at present no general data breach notification requirement in the Directive, although one exists in the EU e-Privacy Directive and, in addition, some individual EU member states (notably, Germany in 2009 and Austria in 2010) have enacted such requirements generally.

[7] Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services, September 1, 2010, Queen Mary, University of London.

Renzo Marchini is Counsel at Dechert LLP, London, and a member of the World Data Protection Report Editorial Board. He is also the author of the book Cloud Computing: A Practical Introduction to the Legal Issues (BSI, November 2010). He is grateful for the useful assistance of James Taylor, Trainee Solicitor at Dechert LLP, London, in the preparation of this article. The author may be contacted at renzo.marchini@dechert.com.