The impact of *Schrems* on data transfers and the cloud

The recent decision of the Court of Justice of the European Union ('CJEU') in the *Schrems*[1] case has stirred up the discussion and concerns with respect to the safety of international data transfers to non-EU countries. João Alfredo Afonso and Leonor Bettencourt Nunes, Partner and Trainee Lawyer respectively at Morais Leitão, Galvão Teles, Soares da Silva & Associados, examine the safety concerns regarding international data transfers that are particularly relevant in the context of cloud computing, and the increasing use of remote servers for the storage and processing of data.

Introduction

In the past years, cloud computing has been gaining increasing relevance in the global market as providing an efficient and cost-saving tool for individuals, companies and even public entities. However, for EU/EEA-based companies and individuals, the main issue is the uncertainty associated with the location of the servers used by many cloud service providers, notably with regards to providers based outside the EU/EEA, which by implicating international transfers may not offer the same guarantee of personal and business data protection as the EU standard.

The EU legal framework

The EU is endowed with a strict privacy law framework, applicable also to the EEA, and essentially contained in the Data Protection Directive 95/46/EC ('the Directive'), which establishes, in Article 25(1), that the transfer of personal data 'may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.' Therefore, cloud providers using non-EU/EEA-based servers which enter into service agreements with EU/EEA-based companies or individuals, must comply with EU privacy law.

The European Commission has powers to assess and decide whether a certain third country provides a level of protection deemed adequate under EU standards, either by reason of its national privacy law framework or in view of any international commitments entered into by that third country. Until the time of writing, only Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US Department of Commerce's Safe Harbor Framework (which has now been overturned by the CJEU ruling) have been recognised as having an adequate level of protection for free international data transfers.

Even though the 'list of adequate countries' is still significantly short, it does not exhaust the options for lawful international transfers of data. The EU legal framework provides for other possible mechanisms available to data controllers and data processors in order to ensure compliance with the EU protection standards.

First of all, the European Commission has adopted three distinct sets of standard contractual clause (the so-called EU Model Clauses): two sets aimed at transfer from controller to controller ('C2C Model Clauses') and another regarding controller to processor transfers ('C2P Model Clauses'), which were revised in 2010. In March 2014, the Article 29 Working Party ('WP29') approved a draft of new model clauses for processor to processor international data transfers; nonetheless, these have not been yet adopted by the European Commission.

Another option, particularly for multinational companies, is the adoption of Binding Corporate Rules ('BCRs') for transfers taking place within the same corporate group. This process implies the drafting of internal rules for intra-group transfers providing adequate safeguards for the protection of personal data in data flows, which then have to be reviewed and authorised by a national data protection authority.

Finally, Article 26 provides a list of derogations under which data may be lawfully transferred to third countries.

The decision in *Schrems*

The case gathered considerable attention as it concerned intra-group international data transfers performed by the social network Facebook from its EU subsidiary, based in Ireland, to its US servers. Mr. Schrems, an Austrian Facebook user, filed a complaint to the Irish Data Protection Commissioner, following the revelations of former CIA agent Edward Snowden that the US National Security Agency ('NSA') had tapped into servers of several American companies, arguing that the recent scandal demonstrated that US law and international commitments, namely the Safe Harbor, did not offer an adequate protection from surveillance by public authorities of individuals and companies.

The High Court of Ireland referenced the case for preliminary ruling by the CJEU on the question of whether a national data protection authority is impeded from examining a complaint on an

international data transfer when there is an adequacy decision by the European Commission. The CJEU considered that national data protection authorities not only are not impeded from but should, in fact, investigate and assess any complaints on international data transfers and went further by declaring invalid the European Commission decision finding that the Safe Harbor granted an adequate level of protection.

The CJEU decision stressed that Safe Harbor is only applicable to the US undertakings that adhere to it and which are obliged to set its protection rules aside for overriding reasons of public interest and national safety which may determine indiscriminate surveillance by US public authorities to EU-based individuals and companies. Finally, the CJEU concluded that the Safe Harbor did not protect the fundamental rights of respect for private life and effective judicial protection, thus declaring the European Commission adequacy decision invalid.

Other recent developments

Following this ruling, the WP29 issued a statement, on 16 October 2015, to reflect a common position on the implementation of the judgement. The WP29 stated that international data transfers taking place under the Safe Harbor decision are considered unlawful. It was further stated that the WP29 would assess the impact of the judgment on other transfer tools by the end of January 2016. However, the group assured that EU model clauses and BCRs can still be used.

The European Commission had already decided to request a revision of Safe Harbor, as well as the Umbrella Agreement (which regulates transfers between the EU and the US for law enforcement purposes), following the Snowden scandal, in order to guarantee higher levels of protection and thus rebuild trust in EU-US data flows. With regards to the Umbrella agreement, the finalisation of the negotiations between the EU and the US was announced, on 8 September 2015, and it is expected that the end of the Safe Harbor negotiations will shortly follow.

Cloud operators wishing to provide services in the EU will have to engage in a review of their legal instruments and protection mechanisms in order to guarantee EU standard safeguards for international data transfers under the cloud

Similarly, these efforts to reassure individuals and companies regarding the protection of their data in cross-border transfers to third countries have also been done on the part of cloud service providers. Recently, Microsoft undertook a revision of its enterprise agreement for the provision of cloud services ('MS Agreement') to incorporate C2P Model Clauses and was the first cloud provider to obtain confirmation[2], from the WP29, of the compliance of its cloud contracts with the EU standards. Nonetheless, the Chairwoman of WP29, Isabelle Falque-Pierrotin, clarified that the review undertaken was only a partial analysis since the Annexes regarding which transfers are covered by the contract could not be properly assessed, since these would have to be reviewed on a case-by-case basis.

Furthermore, the European Commission's proposal for an EU General Data Protection Regulation, which is still pending approval by the European Parliament and Council of the European Union, will reform the legal framework for data protection and create a level-playing field for EU-based companies and individuals - as well as non-EU/EEA-based companies operating in the EU/EEA - by providing a single set of rules applicable to all EU Member States.

It also targets the establishment of a safer environment for international data transfers, by streamlining the approval process of BCRs, and simplifying the national authorisation processes for the processing of personal data, as well as reducing the number of mandatory notifications for data processing (which will be mostly beneficial for SMEs).

Conclusion

Considering the recent developments as well as the data protection reform, which is in the pipeline, it is to be expected that cloud operators wishing to provide services in the EU, will have to engage in a comprehensive review of their legal instruments and protection mechanisms in order to guarantee EU standard safeguards for international data transfers under the cloud. For the time being, the safer approach in terms of legal certainty appears to be the protection of data in international data transfers through the implementation of EU Model Clauses and BCRs.

João Alfredo Afonso Partner
Leonor Bettencourt Nunes Trainee Lawyer
Morais Leitão, Galvão Teles, Soares da Silva & Associados, Portugal
joaoafonso@mlgts.pt
lbnunes@mlgts.pt

1. Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* [2015].
2. By letter of 2 April 2014, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf