WHITE & CASE

Use "Adequate Protection," Avoid I(legally)T(ransmitting)D(ata)

April 2011

Manuel Martinez-Herrera*

White & Case

"Without such a[n adequate protection] finding businesses must undertake more cumbersome and expensive processes under European law to legitimize such data transfers. A finding will be potentially advantageous to New Zealand from a trading perspective."[1]

I(llegally)T(ransmitting) D(ata)

Every day, personal data are transferred across international borders in amounts impossible to quantify. Most companies in the EU/EEA, as in any other region of the world, constantly need to send personal data outside that area for multiple business, administrative and compliance reasons in order to run their day-to-day operations and stay competitive in a market that is a little more global with every day that passes. An Austrian tourism agency that organizes trips to Brazil, for example, needs to send its customers' data to the Brazilian hotels; the Spanish subsidiary of a US company may need to send personal data of its employees, suppliers or customers to the US headquarters; a Japanese NGO trying to collect donations in Europe to help Japan with the terrible consequences of the recent earthquake may need to send donors' personal data outside of Europe, etc.

Despite the vital importance of cross-border data transfers, illegally transmitting data outside the EU/EEA is one of the most usual ways in which companies violate local laws implementing the so-called EU Data Protection Directive[2] and one more reason for corporate compliance officers to suffer yet another headache.

In fact, article 25.1 of the Directive establishes that data transfers to a third country[3] "*(…) may take place only if (…) the third country in question ensures an adequate level of protection.*" A literal interpretation of this provision, and especially of the use of the word "only," would imply that either the third country is a "data-safe destination" under EU standards and data can be freely transmitted there or it is unsafe and no data at all can be transferred unless one of the exceptions included in article 26 apply. Of course, this would make it very complicated to do any business with those "unsafe" jurisdictions which, as we will see, are most of the countries in the world. As a result, the EU developed certain mechanisms

This article was published in a slightly different form in the April 15, 2011 issue of *EuroWatch*

* The author is an International Labor & Employment Law Associate at White & Case LLP, New York. His practice focuses on counseling multinational employers on cross-border human resources and data privacy issues affecting multiple countries and jurisdictions. For review and comments on drafts of this article, the author thanks Donald C. Dowling, Jr. (White & Case, NY).

1 *Report by the [New Zealand's] Privacy Commissioner to the Minister of Justice on the Privacy (Cross-border Information) Amendment Bill* at § 1.4., *available at* http://privacy.org.nz/report-by-the-privacy-commissioner-to-the-minister-of-justice-on-the-privacy-cross-border-information-amendment-bill/

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML*

3 A "third country," for these purposes, is a country outside of the European Economic Area (EEA), which includes the twenty seven EU Member States, Iceland, Liechtenstein and Norway.

Use "Adequate Protection," Avoid I(legally)T(ransmitting)D(ata)

that when properly implemented "sanitize" individual data transfers, as opposed to all collective transfers, to "unsafe" jurisdictions. These are chiefly: the US Safe Harbor Certification, the Standard Contractual Clauses, and Binding Corporate Rules.

This article, however, does not focus on these individual mechanisms,[4] as its primary goal is to explore the history, evolution and future of the "adequate protection" standard that the EU developed as a starting point to identify certain jurisdictions as "data-safe destinations" to which data can be automatically sent from the EU.

The Process

Article 25.6 of the EU Data Protection Directive designates the EU Commission as the institution in charge of determining which countries ensure an adequate level of data protection "*by reason of its domestic law or of the international commitments it has entered into.*" Once the Commission is satisfied about the protection offered by a jurisdiction, it makes its finding public by adopting a "Commission Decision." However, before reaching this final step, there is a whole previous process that includes:[5]

- An initial proposal from the Commission. Often times, the country looking to obtain a positive finding, especially when it does not have a special political or administrative relationship with an EU Member State, will directly request the Commission to start the process through diplomatic channels.[6]
- A positive opinion from the Article 29 Working Party.[7] This is an essential step for any jurisdiction that aspires to obtain a positive finding.
- An opinion from the Article 31 Management Committee[8] delivered by a qualified majority of Member States.
- A thirty days right of scrutiny for the European Parliament (EP) to check if the Commission has used its executing powers correctly. The EP may, if it considers it appropriate, issue a recommendation.
- The adoption of the decision by the Commission.

But any avid reader, or country in search of a positive adequate protection finding, would not only want to know about the formal process, and would wonder what the Commission is really looking for in a country in order to make its determination. In its decisions to date, the Commission has offered some general guidance. The decisions usually refer to an analysis of the local data privacy/protection laws and implementing regulations that the country has enacted and the data privacy conventions, guidelines or other international instruments[9] the country has entered into to see whether these are *"largely based on the standards set out"* in the EU Data Protection Directive,[10] and *"cover all the basic principles necessary for an adequate level of protection for natural persons."*

This, of course, is very broad guidance. The Article 29 Working Party, whose previous opinion, as we have seen, plays a very important role in the process, has provided more specific guidelines. This group has made clear what it is looking for in a candidate:[11] the existence in its legal system of certain *"data protection 'content' principles and 'procedural/enforcement' requirements."*

- The Content Principles: The privacy laws or regulations of a country that may be considered to have adequate data protection need to include the following principles: the purpose of limitation principle; the data quality and proportionality principle; the transparency principle; the security principle; the rights of access,

4 For more information on these mechanisms *see* Donald C. Dowling, Jr. and Jeremy M. Mittman, International Privacy Law, in Proskauer on Privacy (Kristen J. Mathews, ed. 2010), at § 14:3.

5 *See* http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm

6 For example, on October 20, 2008, the Mission of the Eastern Republic of Uruguay to the European Union sent a letter to the European Commission to officially request the Commission to initiate the procedure. *See* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp177_en.pdf

7 The Article 29 Working Party is an independent EU advisory body on data protection and privacy formed by the national data protection commissioners of the EU Member States, the European Data Protection Supervisor and a Commission representative. The Commission also provides the Working Party's secretariat.

8 The Article 31 Management Committee is a group formed by representatives of the Member States and chaired by a representative of the Commission.

9 Such as the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data or the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

10 It is logically easier to obtain a positive finding if the domestic laws are modeled after the EU Data Protection Directive. Out of the nine positive determinations made so far, the Commission found that was the case for six of them (all but Argentina, Canada and Switzerland).

11 *See* Article 29 Working Party's *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* adopted on 24 July 1998, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf

Use "Adequate Protection," Avoid I(legally)T(ransmitting)D(ata)

rectification and opposition; and restrictions on onwards transfers.

- The Procedural/Enforcement Mechanisms: The candidate's data protection procedural system must ensure the following objectives: to deliver a good level of compliance with the rules; to provide support and help to individual data subjects in the exercise of their rights; and to provide appropriate redress to the injured party where rules are not complied with. Complying with these objectives might be easier if there is a supervisory authority, a so-called data protection authority, in charge of enforcing the rights and obligations under the domestic privacy laws.

The Chosen 9

As of March 2011, only nine jurisdictions have received an adequate data protection finding: Switzerland (Commission Decision of 7/26/2000), Canada (12/20/2001), Argentina (6/30/2003), Guernsey (11/21/2003), Isle of Man (4/28/2004), Jersey (5/8/2008), Faroe Islands (3/5/2010), Andorra (10/19/2010), and Israel (01/31/2011).[12]

Switzerland, a historic EU business partner completely surrounded by EU countries and that has a comprehensive data privacy law predating the EU Data Protection Directive by more than three years, was the perfect candidate to be the first country recognized by the Commission as having adequate protection. This happened in July 2000.

At the end of 2001, Canada, another important EU business partner, was the second country to be issued an adequate protection finding just a little over a year after its federal data privacy law, PIPEDA, was enacted. The finding is limited to *"recipients subject to"* PIPEDA. Canada is, to date, the only North American country that forms part of this privileged club. Mexico, based on its recent enactment of an omnibus data protection law, the Federal Law on Protection of Personal Data Held by Private Parties,[13] is the logical candidate to be the next country to enlarge North America's presence in this "data-safe destination" group.

We had to wait until mid 2003 for a South American country, Argentina, to secure a positive decision from the Commission. Argentina's recognition was primarily due to the similarities between its data privacy law and the Directive. Uruguay may probably soon join Argentina as the second South American country with a positive determination.

After these first three decisions validating the data protection standards of three trading partners of a considerable size, more than seven years had to pass until another economically and politically significant jurisdiction, Israel, obtained the Commission's approval at the beginning of 2011. During those seven years only five jurisdictions, all of a considerably smaller size than the first three in terms of population, extension and economic power, were anointed by the Commission as having adequate protection: the three British Crown Dependencies (Guernsey in November 2003, Isle of Man in April 2004 and Jersey in May 2008), the Faroe Islands in March 2010 and Andorra in October 2010. All of these have in common being smaller jurisdictions located in the European continent and having very tight political, administrative and economic relationships with certain EU Members (UK; Denmark; and Spain and France, respectively).

As of April 2011, the Commission has not issued any adequate protection decisions in favor of countries from Africa, Asia or Oceania. The Article 29 Working Party, however, has issued opinions on the level of protection of personal data in New Zealand[14] and Australia.[15] As recently as April 4, 2011, the Article 29 Working Party, despite certain reservations with regard to the regulation of direct marketing and onward transfers, issued a positive opinion in favor of New Zealand. Australia was not as lucky when more than ten years before the same group of experts stated that Australia's regime could only be regarded as adequate *"if appropriate safeguards were introduced to meet"* the specific concerns expressed by the Working Party in its opinion. With this the Working Party was basically telling the Australian government that it needed to improve and strengthen its data privacy regime in order to obtain a positive finding from the Commission.

The Candidates

For an array of reasons, Uruguay is, without a doubt, the number one candidate to be the next jurisdiction to obtain an adequate protection finding. Uruguay's data protection law is very similar to Argentina's, a legal regime already approved by the Commission, and the Article

12 All the decisions from the Commission are *available at http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm*

13 For more information on Mexico's recent data privacy law *see* Manuel Martinez-Herrera, *The 2010 Top 10 EU Data Privacy Changes*, EuroWatch, Vol. 23, No. 2 (2011).

14 *See* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp182_en.pdf

15 *See* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp40en.pdf

Use "Adequate Protection," Avoid I(legally)T(ransmitting)D(ata)

29 Working Party already issued its affirmative opinion in October 2010.[16] Therefore, everything indicates that the Commission decision in favor of Uruguay could be issued sometime during 2011. New Zealand is, due to the very recent opinion from the Working Party, the second serious contestant with possibilities to be anointed by the Commission in the near future.

Other potential candidates include countries that have recently enacted or amended comprehensive data privacy laws such as Mexico, Morocco and Ukraine. Malaysia and Taiwan may also become candidates once their recently passed law and amendment (respectively) enter into force.[17] However, as we will explain, it might take more time than usual for these countries to have a chance to obtain such recognition due to the privacy regime reform process that the EU is currently undertaking.

Why Does It Matter or Why Does It Not?

The words from New Zealand's Privacy Commissioner reproduced at the beginning of this article are the best answer to the first of these questions: *"Without such a[n adequate protection] finding businesses must undertake more cumbersome and expensive processes under European law to legitimize such data transfers. A finding will be potentially advantageous to New Zealand from a trading perspective."* That is to say, obtaining such recognition from the Commission should be, in principle, economically advantageous for a jurisdiction as, once anointed, companies based in the EU/EEA would be able to freely send personal data to such jurisdiction as if sent within the EU/EEA area (e.g., a transfer from Spain to Argentina is considered the same as a transfer from Spain to Denmark) without having to use model contractual clauses, binding corporate rules, etc. This, of course, simplifies the transfer, makes it cheaper and makes the jurisdiction a more appealing destination for EU/EEA-based businesses to grow there either directly by opening new subsidiaries or branches or indirectly through the outsourcing of part of their business.

This appears to be the rationale shared by the countries that decided to jump onto the EU comprehensive data protection regime wagon, as the information published by "Uruguay XXI," the Uruguayan Investment and Export Promotion Institute, also evidences: *"The EU recognition will open the possibility for major European investments, in particular it will help Uruguay boost its outsourcing industry (call centers, data centers, technology parks) and attract more EU-based companies looking for providers of administrative, financial and other data processing services in Latin America."*[18]

That being the case, why have only a very limited number of countries tried to obtain adequate protection recognition? As we have seen, only nine jurisdictions, five of which have a population of less than 100,000, out of the more of one hundred ninety countries in the world, have been anointed by the Commission, and only two more jurisdictions, Uruguay and New Zealand, are currently under serious consideration. We can all agree that this is not a significant turnover for the more than fifteen years that the Directive has been in force.

The explanation to this might be twofold:

- Implementing an EU-style data protection regime is a lengthy, expensive, burdensome and potentially contested undertaking from the political, legislative, administrative and enforcement perspectives. Legislators from many jurisdictions may consider this task daunting and maybe also unnecessary as individual data controllers have other mechanisms (e.g., US Safe Harbor Certification, Standard Contractual Clauses, Binding Corporate Rules) they can effectively use to privately comply with the EU international data transfer requirements without the specific data importing jurisdiction having to make the effort to adjust to the strict EU data protection parameters to obtain adequate data protection recognition.
- The implementation by a country of an omnibus data protection regime that may be deemed as offering adequate data protection by the European Commission may act as a deterrent for new businesses to start operations. It is arguably cheaper for companies to operate in a less-privacy-regulated environment

16 *See* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp177_en.pdf

17 For more information on these recent enactments or amendments *see* Manuel Martinez-Herrera, *The 2010 Top 10 EU Data Privacy Changes*, EuroWatch, Vol. 23, No. 2 (2011).

18 *See* http://www.uruguayxxi.gub.uy/innovaportal/v/1315/2/innova.front/uruguay_recognized_by_the_european_union_as_offering_an_adequate_level_of_data_protection

where they do not have to allocate resources to, for example, notifying data subjects, differentiating the treatment of sensitive data from regular data, transferring data abroad, purging obsolete data, etc. That is to say, the same economic/trading analysis that may make a country consider it beneficial to implement a robust data privacy regime in order to be anointed by the Commission may be used to argue that less regulation makes more business sense.

Looking Ahead

As is widely known, the Commission is currently embarked on a process to reform the EU data privacy legal framework. As part of this reform, the Commission[19] has already declared that it intends to *"improve, strengthen and streamline the current procedures for international data transfers, including the so-called 'adequacy procedure.'"*

Based on the information released so far, the reform will not only be limited to new requirements or limitations concerning international data transfers; it is conceived as a global reform of the EU privacy legal system. The Article 29 Working Party[20] and the Commission's positions appear to suggest the EU might be moving towards an even less business-friendly data privacy regime with the proposed inclusion of new individual rights for data subjects, such as the "right to be forgotten" or a data breach notice right.

Therefore, it is within the realm of possibilities that no new countries, with the possible exceptions of Uruguay and New Zealand as they have already been vetted by the Article 29 Working Party, will obtain an adequate data protection finding until the reform process is completed which may well take several years. It would not make much sense for the Commission to use the "adequate protection" process when it is currently under scrutiny and likely to be somewhat reformed to approve jurisdictions whose data protection level may be "adequate" under current EU standards, but deficient once the reform has been completed.

19 *See Data protection reform – frequently asked questions* press release dated November 4, 2010, *available at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/542*

20 *See* Article 29 Working Party's *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* adopted on December 1, 2009, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Manuel Martinez-Herrera *is an International Labor & Employment Law Associate at White & Case LLP, New York. His practice focuses on counseling multinational employers on cross-border human resources and data privacy issues affecting multiple countries and jurisdictions.*

The information in this article is for educational purposes only; it should not be construed as legal advice.