HACIA UN NUEVO DERECHO EUROPEO DE PROTECCIÓN DE DATOS

TOWARDS A NEW EUROPEAN DATA PROTECTION REGIME

Artemi Rallo Lombarte
Rosario García Mahamut
Editores

tirant lo blanch
Valencia, 2015

The european data protection adequacy decision and its effects on third countries. A failed and inadequate standard for Latin America

Cristos Velasco

*Founder of Protección Datos México (ProtDataMx)**

1. INTRODUCTION

Without doubt, Europe has the most comprehensive and restrictive legal framework in the field of data protection, which together with the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data better known *as 'Convention 108'*[1] and the OECD Guidelines on the Protection of Privacy and Transborder Flows

---

* http://protecciondatos.mx Further info about the author at: http://protecciondatos.mx/about-the-founder/?lang=en. Special thanks to Eduardo Ustaran, partner at Hogan Lovells for his kind feedback and comments on preliminary drafts of this article.

1 The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (Convention 108) was the first international treaty dealing with the protection of personal data and privacy as fundamental human rights in the automatic processing of data. The Convention opened for signature on 28 January 1981 and has been extended for signature and ratification to other countries. Convention 108 is supplemented by an additional Protocol regarding supervisory authorities and transborder data flow. Convention 108 is currently going through a modernization process in order for such treaty to catch up with the advancements in technology and in particular to regulate how data is used, processed, shared and exchanged outside Europe and through the use of platforms and services in the context of cloud computing platforms. For further reference and documents on the modernization process of Convention 108, see the website of the Council of Europe at: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

of Personal Data[2] have been used as model inspiration in many countries around the world for the drafting of data protection legislation and policies, which includes most of the countries of the Latin American region.

In October 1995, the European Parliament and the Council of the European Union enacted Directive 95/46 (EC) on the protection of individuals with regard to the processing on personal data and the movement of such data better known as the *"EU Data Protection Directive"*, which fully came into effect on October 25, 1998[3]. The EU Data Protection Directive was one of the key instruments in seeking to harmonize data protection legislation across the EU Members States in order to protect the right to privacy of individuals with respect to it processing of personal information.

Since the end of the nineties, the European Union has exported its regulatory data protection model to other countries around the globe so that it could ensure the adoption of an effective data protection legal regime based on the European Data Protection

---

2 The OECD Privacy Guidelines is an international non-binding regulatory standard approved in 1980 that establishes a set of national and international principles on data protection that have been used in many countries around the world to enact privacy and data protection legislation including the regulation of transborder data flows. The OECD Privacy Guidelines went through a revision process in January 2013 as part of the different activities conducted in the context of its 30th anniversary. The revisions conducted by a group of experts of the OECD leave without any modifications the original basic principles of the guidelines. The OECD mainly focused its work in introducing new themes and concepts that countries should focus their attention to, namely national privacy strategies, privacy security programs and data security breach notification. See the website of the OECD 2013 Privacy Guidelines at:
http://www.oecd.org/sti/ieconomy/privacy.htm#newguidelines

3 Directive 95/46 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 of the free movement of such data published in the Official Journal of the European Union núm. 281 of 23/11/1995, available at: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

Directive and the assessment of the European Commission on whether a country outside Europe and the European Economic Area has legislation in place that provides an *"adequate level of protection"*[4] to the EU Data Protection Directive for the purpose of transferring and processing of personal data outside Europe[5].

The EU Data Protection Directive was a very innovative regulation at the end of the nineties considering that it was one of the very few existent legal binding instruments that other countries could use as a reference to draft data protection legislation. Unfortunately, a number of countries including some of Latin America copied the European model without foreseeing the political and trade implications that come within its implementation, including the unintended regulatory burdens and unnecessary bureaucracies for companies to comply with the laws and the adequacy decision regime of the European Commission as a de facto standard to follow.

According to Christopher Kuner, a German expert on data protection law, *"restricting data transfers to non-adequate countries seems not be considered a fundamental principle of data protection law"*. In his view, the concept serves a political end to prevent circumvention of the EU law rather than being a principle of data pro-

---

4 The term *"adequate level of protection"* is not defined in the EU Data Protection Directive. The guidelines and criteria to asses the data protection level in third countries have been defined by the predecessor of the Article 29 Working Party in two documents: (1) Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, "*First orientations on Transfer of Personal Data to Third Countries. Possible Ways Forward in Assessing Adequacy"*. Discussion Document adopted by the Working Party on 26 June 1997, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf and (2) Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *"Transfers of personal data to third countries: Applying Article 25 and 26 of the EU data protection directive"*. Working document adopted by the Working Party on 24 July 1998, available at:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf

5 See Article 25 of the EU Data Protection Directive 95/46/EC.

cessing in itself and in his opinion, there are other more efficient ways to prevent circumvention of EU law rather than promoting the adequacy concept[6].

Sixteen years have passed since the adoption of the EU Data Protection Directive and there is the shared view among policy makers, data protection authorities and experts around the world that the EU Data Protection Directive not only has created obstacles and complex procedures for multinational companies and organizations to achieve compliance in the European market, but in particular, the Directive has since been superseded by trends and changes in technology, particularly the way that data is now exchanged, processed and moved across borders trough the use of social networks and Internet based platforms[7].

The main question that we seek to give an answer to in this article is whether the European Union should continue to export its adequacy decision model on data protection to other countries considering the burdens to both, data protection authorities enforcing the laws and regulations and multinational companies seeking to comply with them, but particularly whether governments of Latin America countries should allow the imposition of the adequacy decision standard by the European Commission in their national legal systems.

Before proceeding to the analysis of the content of this article, it is worth mentioning that the adequacy decision procedures conducted by the EU Commission could possibly lead to international trade issues and disputes in some regions, and even some countries might even raise issues of national sovereignty under

---

6 Kuner, Christopher, *"Developing an Adequate Legal Framework for International Data Transfers"* Springer Science + Business Media B.V. 2009, electronic copy available in the website of the Social Science Research Network, p. 5.

7 See: Rudgard, Sian, *"Origin and Historical Context of Data Protection Law"* in *European Privacy. Law and Practice for Data Protection Professionals*, International Association of Privacy Professionals (IAPP), Chapter One, 2012, p. 13.

public international law based on the principle of non- intervention, alleging the right to independence and sovereignty of the State and the prohibition of foreign countries or regional organizations to intervene in their internal or legal affairs. The adequacy decision procedure between the European Commission and States outside the EU seeking to reform or creating legal frameworks for international data transfers and data flows in their corresponding data protection legislation might create unnecessary tensions and disputes in the future.

The Data Protection Regulation of the European Commission was originally proposed in January 2012 and despite all the changes and reform proposals as a result of the lobbying of influential American technology companies in Brussels, the Data Protection Regulation received strong support by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs with an overwhelming majority and it has also been widely discussed by national Ministers in the Justice Council[8].

Unfortunately, the proposed Data Protection Regulation of the European Commission continues to include the *"adequacy decision standard"* that has been very controversial from both, a regulatory and trade perspective especially for countries in Latin America like Mexico, Chile, Colombia and Peru that have a solid network of commercial treaties with countries like the United States, Canada[9] and with countries of the Asia-Pacific region where the flows

---

8 See European Commission Memo: *"Data Protection Day 2014: Full Speed on Data Protection Reform"*, Brussels, MEMO/ 14/60, 27 January 2014, available at: http://europa.eu/rapid/press-release_MEMO-14-60_en.htm For an academic contribution containing a legal analysis of the original European Commission Data Protection Regulation proposal and the amendments adopted by the European Parliament, see Cuijpers, Colette, Purtova, N. & Kosta E., *"Data Protection Reform and the Internet: The Draft Data Protection Regulation"*. Tilburg Law School Legal Studies Research Paper Series núm. 03/2014 available in the website of the Social Science Research Network.

9 *See* Bennet, Colin and Charles Raab, "*The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response"* The Information Society. An International Journal, Volume 3, Issue 3, 1997.

of data across borders play an important role in the hegemony of commercial trade, investment, and the possibility of innovating ideas, creating new business opportunities and projects that require the exchange of information and data among Internet based businesses located in those countries.

The first section of this article provides a background of the adequacy standard in Europe contained in the EU Data Protection Directive and takes a brief look at the countries that have met such adequacy standard. The second section contains an analysis of Chapter Five of the proposed Data Protection Regulation, which sets out the conditions, alternatives and exemptions for the transfer of personal data to third countries or international organizations. The third section reviews on a comparative basis the international and regional instruments containing provisions regulating transborder data flows. The fourth section looks at the emerging mechanisms for the transfer of cross-border data created in the context of regional organizations an in particular in the context of APEC, and reviews the existing mechanisms that countries might follow for the transfer of data across borders. Since the purpose of this paper is to make policymakers, data protection authorities and experts in Latin America aware of the regulatory burden of the *"adequacy decision standard"*, section five analyzes the countries in Latin America whose data protection legislation has been deemed as providing an *"adequate level of protection"* by the European Commission and the current regulation of international data transfers in four countries of Latin America that have data protection laws and regulations in force. We finalize this paper by enlisting conclusions and proposals that countries of the Latin American region might use in order to export data to the EU without having to meet the onerous *"adequacy decision standard"* required by the European Commission in the proposed Data Protection Regulation.

2. BACKGROUND OF THE ADEQUACY STANDARD IN THE EUROPEAN UNION

The adequacy decision standard has its roots in the EU Data Protection Directive[10]. Chapter IV consisting of Articles 25 and 26 set out the current rules for the transfer of personal data to third countries[11].

Article 25(1) establishes that the transfer of personal data, which are undergoing processing or intended for processing might take place only if the third country in question ensures an adequate level of protection.

Article 25(2) sets out the criteria and how the adequacy level of protection of a third country shall be assessed. First, such assessment shall be conducted by taking into account the circumstances surrounding a set of data transfer operations. Second, giving particular considerations to the nature of the data and the purpose and duration of the proposed processing operations. Third, taking into account the country of origin and country of final destination. Fourth, considering the rule of law, both general and sectoral, in force in the third country in question; and fifth, the professional rules and security measures which are complied with in that country.

Article 25(3) allows Member Sates and the Commission to inform each other of cases where they consider that a third country does not ensure an adequate level of protection.

Article 25(4) sets out the power of Member States to take the necessary measures to prevent any transfer of data to third countries when the EU Commission finds that the third country in question does not ensure an adequate level of protection.

Article 25(5) allows the EU Commission to enter into negotiations with a view to remedying the situation resulting from the finding contained in paragraph 4 that a third country has not ensured an adequate level of protection.

---

10 *See* note 3.

11 For an analysis on transboundary data flows in Europe and its extraterritorial effects, see Poullet, Yves, *"Transborder Data Flows and Extraterritoriality: The European Union Position"*, CRID March 21, 2007, pp. 6-10.

Article 25(6) establishes the mechanism that the EU Commission should follow when a third country has ensured an adequate level of protection by reason of its domestic law or of the international commitments entered to for the protection of private lives and basic freedoms and rights of individuals.

The adoption of the European Commission adequacy decision is based on Article 25.6 of the Data Protection Directive, which involves a lengthy administrative process that includes: (i) a formal proposal from the European Commission; (ii) an opinion of the group of the national data protection commissioners through Article 29 Working Party[12]; (iii) an opinion of the Article 31 Management committee delivered by a qualified majority of Member States; (iv) a thirty-day right of scrutiny for the European Parliament, to check if the European Commission has used its executing powers correctly. The European Parliament may, if it considers it appropriate, issue a recommendation; and (v) the adoption of the decision by the College of Commissioners.

Adequacy findings by the European Commission have binding effects across the EU membership. When the European Commission publishes an adequacy finding for a certain country in the Official Journal of the European Union, all members of the European Economic Area, including Norway, Liechtenstein and Iceland and their respective internal administrative organs are bound to follow the decision, meaning that data can flow from the European Union to the country declared as adequate without car-

---

12 The Article 29 Data Protection Working Party was established under the EU Data Protection Directive as an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46 EC and Article 15 of Directive 2002/58/EC and it functions under a set of rules of procedure approved on 15 February 2010. It is composed of: (i) a representative of the supervisory authority (ies) designated by each EU country; (ii) a representative of the authority (ies) established for the EU institutions and bodies; (iii) a representative of the European Commission. The website of Article 29 DPWP is available at: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

rying out prior checking or licensing procedures before national authorities or without any further safeguard.

The European Commission has so far recognized 12 countries: Andorra, Argentina, Australia, Canada (limited to the sphere of commercial organizations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay and the US Department of Commerce's Safe Harbour Privacy Principles (covering companies that have voluntarily joined and endorsed the principles) as providing adequate protection to the EU Data Protection Directive[13].

One of the major critics of the adequacy model of the European Commission is that it is a slow, complicated and lengthy process and it could take many years for the remaining countries in the world to be found adequate[14].

Besides, the adequacy decision formality, the EU Data Protection Directive stipulates in its Article 26 other possibilities as legal grounds for the international transfers of personal data to third countries, which do not ensure an adequate level of protection of data. The situations for the transfers of data to non-adequate jurisdictions are the following:

1. *That the transfer of data might take place subject to the condition that: (i) the data subject has given his consent unambiguously to the proposed transfer; or (ii) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre contractual measures taken in response to the data subject's re-*

---

13 The EU Commission and the Council's Decisions, Opinions of the Article 29 Working Party, Safe Harbour documents, reports and agreements on Transfer of Name Passenger Records with the 12 countries, including with the United States are available in the website of the European Commission at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

14 KUNER, Christopher, *"Developing an Adequate Legal Framework for International Data Transfers", op. cit.*, note 6, pp. 3-4.

quest; or (iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (iv) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or (v) the transfer is necessary in order to protect the vital interests of the data subject; or (vi) the transfer is made from a register intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest to the extent that the conditions laid down in law for consultation are fulfilled in the particular case[15].

2. *The signature of EU standard contractual clauses between the data exporter and the data importer. This means that companies or data controllers might enter contracts between them specifying the company or data controller sending the data and the non-EU company receiving the data. The contract should contain measures and adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights within the meaning of the EU Data Protection Directive*[16].

3. *Pursuant to Article 26 (4), when the European Commission decides that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the decision of the European Commission*[17].

---

15 Article 26 (1) EU Data Protection Directive.

16 Article 26 (2) EU Data Protection Directive.

17 On 15 June 2001, the European Commission adopted Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, Official Journal of the EU/Legislation (OJL) 181/19 of 4 July 2001 available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031:en:PDF This decision was amended by another decision of 27 December 2004, which includes a sec-

Although standard contractual clauses have become relevant alternative mechanisms for the transfer of data from Europe to third countries, its scope will not be the subject of analysis in this article[18].

3. THE ADEQUACY DECISION STANDARD IN THE PROPOSED DATA PROTECTION REGULATION

The original proposal of the Data Protection Regulation of the European Commission of January 2012[19], the latest text of which was formally adopted by the European Parliament on March 12, 2014 seeks to create one single regulation to be enforced by the

---

ond version to the sets of standard contractual clauses that can be used to legitimize international transfers between data controllers, see: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, Official Journal of the EU/ Legislation (OJL) 385/74 of 29 December 2004 available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:en:PDF

18 For Information and the Decisions of the European Commission regarding model contracts and standard contractual clauses for the transfer of personal data to third countries, see the website of the European Commission at http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm For specific information on how adequacy model contracts and standard contractual clauses work in practice, see: USTARAN, Eduardo, *"International Data Transfers"* in *European Privacy. Law and Practice for Data Protection Professionals*, International Association of Privacy Professionals (IAPP), Chapter Twelve, pp. 178-184.

19 Proposal for a Regulation 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 (General Data Protection Regulation) COM (2012) 11 final of 25 January 2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

data protection agencies and supervisory authorities of the 28 Member States[20].

One of the sections that remained unchanged in the original Data Protection Regulation of the European Commission is Chapter V consisting of Articles 40 to 45, which sets out the conditions for the transfer of personal data to third countries or international organizations. The procedures and conditions laid down in that chapter are, at least more descriptive than the provisions on international data transfer of the EU Data Protection Directive, but they continue to put a strong emphasis on the adequacy decision standard for international data transfers to third countries and the conduction of the internal examination procedure by the European Commission. The provisions of this chapter are the following:

Article 40 stipulates that any transfer of personal data, which are undergoing processing or are intended for processing after transfer to a third country or to an international organization may only take place subject to other provisions of the Regulation, and the conditions laid down in chapter five are complied by the controller and processor, including from onward transfers of personal data from the third country or an international organization to another third country or to another international organization.

The criteria, conditions and procedures for the adoption of an adequacy decision by the European Commission, which is largely based in the text of Article 25 of the EU Data Protection Directive is contained in eight subsections of Article 41. The first subsection establishes that a transfer may take place only where the Commission has decided that the third country, a territory or a processing sector within that third country or an international organization ensures an adequate level of protection. Such transfer shall not require prior authorization. The second subsection stipulates that

---

[20] See European Commission Memo/14/186 of March 12, 2014, *"Progress on EU data protection reform now irreversible following European Parliament vote"* available at http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

the European Commission shall give consideration to the following elements when assessing the adequacy of the level of protection: (i) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defense, national security and criminal law, the professional rules and security measures which are complied within that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the EU whose personal data are being transferred; (ii) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organization in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the EU and of Member States; and (iii) the international commitments the third country or international organization in question has entered into.

The third subsection stipulates that the European Commission may decide on the adequacy level of protection of a third country, territory, processing sector or international organization in accordance with the examination procedure provided in Article 87(2) that refers to the application of Article 5 of the EU Regulation No. 182/2011 which enlists the examination procedure for acts to be adopted on a proposal for the European Commission[21].

The fourth subsection stipulates that the implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.

---

[21] Regulation EU 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32011R0182.

The fifth subsection establishes that the European Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organization does not ensure an adequate level of protection within the meaning of paragraph 2 of Article 41, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organization, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3) of the EU Regulation No. 182/2011

The sixth subsection, establishes that when the European Commission prohibits the transfer of any personal data to the third country, or a territory or a processing sector within that third country, or the international organization, provides the possibility of the European Commission to enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of Article 41.

The seventh subsection laid down the obligation of the European Commission to publish a list of those third countries, territories and processing sectors within a third country and international organizations in the Official Journal of the European Union where it has decided that an adequate level of protection is or is not ensured.

Subsection eight stipulates that the decisions adopted by the European Commission on the basis of Article 25(6) or Article 26(4) of the EU Data Protection Directive shall remain in force, until amended, replaced or repealed by the European Commission.

Article 42 sets forth the conditions for transfers to third countries by way of appropriate safeguards, where the European Commission has taken no adequacy decision pursuant to Article 41. The controller or processor may transfer personal data to a third country or international organization only when they have established appropriate safeguards with respect to the protection of personal data in a legal binding instrument. The safeguards referred to in this article are: (i) binding corporate rules in accordance with Article 43; (ii) standard data protection clauses adopted by the European Commission and in accordance with the examination procedure contained in Article 87 (2), which refers to Article 5 of the EU Regulation No. 182/2011; or (iii) standard protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the European Commission pursuant to point (b) of Article 62 (1); or (iv) contractual clauses between the controller or the processor and the recipient of the data authorized by a supervisory authority in accordance with paragraph 4.

Pursuant to subsection three, a transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorization.

Section fourth establishes that where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this article, the controller or processor shall obtain prior authorization of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities, which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

Pursuant to section fifth, where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor

shall obtain prior authorization for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorization by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities, which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.

Pursuant the last section, authorizations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.

Article 43 describes in further detail the conditions for transfers by way of binding corporate rules, based on the current practices and requirements of supervisory authorities. Under this provision, a supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules provided that they: (i) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees; (II) expressly confer enforceable rights on data subjects; (iii) fulfill the requirements laid down in paragraph 2.

Paragraph second establish that the binding corporate rules shall at least specify:

(a) the structure and contact details of the group of undertakings and its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, pro-

cessing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;

(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that a member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;

(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;

(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;

(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;

(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority

the results of the verifications of the measures referred to in point (i) of this paragraph.

Paragraph third empowers the European Commission to adopt delegated acts in accordance with Article 86, for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of Article 43, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.

Paragraph fourth provides that the European Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2), which refers to Article 5 of the EU Regulation No. 182/2011.

Article 44 sets out and clarifies the derogations for data transfers, which are largely based on the existing provisions of Article 26 of Directive 95/46/EC. Pursuant to this article, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or

(d) the transfer is necessary for important grounds of public interest; or

(e) the transfer is necessary for the establishment, exercise or defense of legal claims; or

(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or

(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or

(h) 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.

According to the European Commission, these exemptions apply in particular to data transfers required and necessary for the protection of important grounds of public interest, for example in cases of international data transfers between competition authorities, tax or customs administrations, or between services competent for social security matters or for fisheries management. In addition, a data transfer may, under limited circumstances, be justified on a legitimate interest of the controller or processor, but only after having assessed and documented the circumstances of that transfer operation[22].

Finally, Article 45 explicitly provides in four subsections international co-operation mechanisms for the protection of personal

---

[22] *Op. cit.*, note 19, pp. 11-12.

data. The four subsections mandate the following: (i) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data; (ii) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; (iii) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data; and (iv) promote the exchange and documentation of personal data protection legislation and practice.

Paragraph second stipulates that the European Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).

There is no doubt that the move from a Directive to a Regulation will certainly bring a number of advantages to European countries, one of them is to make it simple for European based companies and organizations to comply with laws and criteria in the enforcement of data protection through the so called "one-stop shop", whereby a single data protection authority will be responsible for an entity or organization operating in different countries of the EU. However the procedure for *"adequacy decisions"* has been maintained in the proposed Data Protection Regulation while giving priority and extending the use of binding corporate rules and contracting legal clauses to legitimize cross-border transfers[23].

After having analyzed the provisions on international data transfers contained in the proposed Data Protection Regulation,

---

[23] See: Sullivan, Clare, *"Protecting digital identity in the cloud: Regulating cross-border data disclosure"*. Computer Law and Security Review (30), 2014, pp. 147-148 electronic copy available in the website of the Social Science Research Network.

we can partially conclude that the provisions for adequacy decision to third countries have been only strengthened. The only changes that we have perceived is that the procedures to transfer data either by way of binding corporate rules or through standard protection clauses adopted by the European Commission or a supervisory authority or through contractual clauses between controllers or processors have been clarified pursuant to the experience in the adoption of said instruments across Europe. Nevertheless, we firmly believe that the supervisory mechanisms and the prior authorization procedure for international data transfers set out in chapter five are still burdensome and do not allow a margin of flexibility specially for countries with little or no experience in the implementation of binding corporate rules and standard data protection clauses.

It should be kept in mind that the great majority of data protection agencies around the world, particularly in Latin America have neither the expertise nor the corresponding specialized units in place to follow up the compliance mechanisms of binding corporate rules or standard protection clauses in addition to the usual shortage of human and financial resources, which clearly might be impediments to follow up their compliance with the corresponding data protection authorities in Europe.

4. THE REGULATION OF TRANSBORDER DATA FLOWS IN INTERNATIONAL AND REGIONAL INSTRUMENTS

The regulation of national and international flows and data transfers is contained in a number of international and regional instruments some of which are binding and others are used as a source of secondary regulation with non-binding effects among countries, but when countries endorse them, they are strongly committed to implement and follow the principles or recommen-

dations contained therein[24]. In this section, we will review the provisions regulating transborder data flows in the current international and regional instruments.

4.1. The OECD Privacy Guidelines

The first international instrument dealing with the regulation of transborder data flows were the OECD Privacy Guidelines of 1980[25] which apply to the processing of personal data for the public and private sector. Part Four of the revised Privacy Guidelines contain a set of basic principles of international application regarding free flow and legitimate restrictions. These principles are:

> *"Paragraph 16. A data controller remains accountable for personal data under its control without regard to the location of the data".*
>
> *"Paragraph 17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines".*
>
> *"Paragraph 18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing".*

The revised OECD Privacy Guidelines includes an important recommendation contained in Paragraph 17 that urges member and non-member countries to avoid measures that restrict or limit the flow of personal data when the are sufficient legal safeguards and enforcement mechanisms in place by the data controllers to ensure a continuing level of data protection. In other words,

---

[24] For a comprehensive study on the legal status of international regulation of transborder data flows under privacy and data protection laws of some countries around the world, see: Kuner, Christopher, *"Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future"*, OECD Digital Economy Paper, núm. 187 OECD publishing 2011.

[25] See *note* 2. The text of the revised OECD Privacy Guidelines is available at: http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

countries shall make sure to have data protection legal framework in place establishing obligations and sufficient safeguards by data controllers to protect the processing and exchange of personal data among different countries but that do not necessarily need the adoption of the European adequacy model.

4.2. The United Nations Guidelines concerning Computerized Personal Files

Nearly 10 years after the publication of the original OECD Privacy Guidelines, the United Nations issued its guidelines concerning Computerized Personal Files, which are applicable to public and private computerized files, including manual files subject to appropriate adjustments[26].

The UN Guidelines are a non-binding document that contains recommendations to be followed by UN country members. Principle 9 of the guidelines contains a recommendation on transborder data flows, which provides the following:

> *"9. Transborder Data Flows*
> *When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands".*

The principle contained in the UN Guidelines is based on the international principle of reciprocity whereby countries are committed to have legal safeguards in place for the protection on privacy and the free circulation of data inside their respective territories.

---

[26] The Guidelines for the Regulation of Computerized Personal Data Files were adopted by the UN General Assembly Resolution 45/95 of 14 December 1990, available at: http://www.refworld.org/docid/3ddcafaac.html

4.3. The Council of Europe Convention 108 and its Additional Protocol

The Council of Europe adopted in January 1981, Convention for the Protection of individuals with regard to the automatic processing of personal data, better known as *'Convention 108'*[27], which is the only existing international binding treaty that seeks to provide guarantees to individuals on the collection and automatic processing of their personal data and the corresponding rights to access, rectification, correction or opposition to the processing of personal information[28].

Chapter III consisting of Article 12 of *Convention 108* contains rules on transborder flows of personal data, whose first paragraph establish prohibitions and authorization conditions for transborder data flows going to the territory of a Member Party. The second paragraph of said article enlists exceptions for the automatic processing of personal data files where the regulations of the other party provide an equivalent protection and when the transfer of data is made from the territory to the territory of a non-contracting State using an intermediary for purposes of circumventing the legislation.

---

[27] Convention for the Protection of individuals with regard to the automatic processing of personal data CETS núm.: 108 has been in force since 1 October 1985, available at http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm As of the writing of this paper, such convention has been ratified by 46 countries. Uruguay ratified it on April 10, 2013 and is the only country of Latin America that has formally accessed and ratified such instrument.

[28] Some academics have argued that Convention 108 and its Additional Protocol will not become an accepted international global privacy treaty in the future unless the Council of Europe takes further steps to promote the advantages of accession to the rest of the countries that are not yet parties, make the policies more transparent regarding the standards that must be met for accession and clarify the procedures to be followed for-non European countries, see: Greenleaf, Graham, *"The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108?"* University of Edinburgh School of Law, Research Paper Series núm. 2012/12, pp. 32-34.

Likewise, Convention 108 seeks to regulate and impose restrictions on transborder flows of personal data to States or third countries where the data protection legislation does not provide equivalent protection, which are further developed in an Additional Protocol that opened for signature in 2001[29].

Article 2 of the Additional Protocol stipulates rules for transborder flows to personal data to countries that are not subject to the jurisdiction of a Member party to the Convention.

Section 1 stipulates that each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

Section 2 allows for the transfer of personal data to third countries where there is no adequate data protection, as long as: (a) the transfer is provided for by domestic law and is necessary for: (i) the specific interests of the data subject; or (ii) legitimate prevailing interests of others, especially important public interest or (b) if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.

Like the European Data Protection Directive, Convention 108 and its Additional Protocol contain a standard procedure that allow member parties to establish legal regimes for transborder data flows to third countries that do no ensure an adequate level of protection, including the use of safeguards which can take the

---

[29] Additional Protocol to Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Supervisory Authorities and Transborder Data Flows has been in force since 1 July 2004. As of the writing of this article, the Additional Protocol has been signed by 43 countries followed by accession and ratification by only 35 countries. Outside Europe, only Uruguay has accessed the Additional Protocol on 10 April 2013. The Additional Protocol is available at: http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm.

form of contractual clauses by data controllers responsible for the transfer of data and the corresponding approval of the national competent authorities.

4.4. The APEC Privacy Framework

The Asia-Pacific Economic Cooperation Forum, which is now composed of 21 member economies approved the *"APEC Privacy Framework"*[30] in 2005, which is a voluntary, non-binding document that recognizes the importance of the development of effective privacy protection in electronic commerce, seeks to avoid barriers to information flows, and ensure continue trade and economic growth in the Asia-Pacific region. The APEC Privacy Framework was largely based on the concepts, values and principles contained in the 1980 OECD Privacy Guidelines but giving particular emphasis on the balance of information privacy with business needs and commercial interest while at the same time seeking to recognize cultural and social diversities that exist between APEC member economies.

The APEC Privacy Framework recognizes *inter alia*, the importance of the free flow of information as an essential element for both, develop and developing market economies to sustain economic social growth and advancing international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among member economies and with their trading partners[31].

One of the core principles of the APEC Privacy Framework is the principle of *Accountability* for domestic and international transfers of data. Such principle sets out that when personal information is to be transferred to another person or organiza-

---

30 The APEC Privacy Framework is available at: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

31 See APEC Privacy Framework, section number 8.

tion, the controller shall obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information complying with each of the privacy principles of the APEC Privacy Framework[32].

The APEC Privacy Framework relies on the use and acceptance of its Cross-Border Privacy Rules (CBPR) system, which is a set of voluntarily rules enacted on 13 November 2011 whereby the privacy policies and practices of companies and organizations are subject to a certification by a third party that will ensure that said companies or organizations are in compliance with the APEC Privacy Framework. The CBPR sets out mechanisms for the mutual recognition and acceptance of rules for international transfers of data without the need for member economies to enact barriers to cross-border trade and information flows including unnecessary administrative and bureaucratic burdens for business and consumers[33].

4.5. International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution)

In November 2009, the Spanish Data Protection Agency introduced a document entitled: *International Standards on the Protection of Personal Data and Privacy*, better known as the *"Madrid Resolution"* during the closing session of the Thirty First International

---

32 See APEC Privacy Framework, section number 26.

33 See APEC Privacy Framework, section number 48 and *APEC Cross-Border Privacy Rules System. Policies, Rules and Guidelines*. This document contains a description of the functioning of the APEC CBPR System and the roles and responsibilities of participating organizations, Accountability Agents and APEC Economies, available at: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx So far only three countries have endorsed and accept APEC's Cross-Border Privacy Rules: USA in July 2012, Mexico in January 2013 and more recently Japan in May 2014.

Conference on Data Protection and Privacy Commissioners held in Madrid on 4-6 November 2009[34].

The Madrid Resolution contains a set of principles and recommendations largely based on the framework contained in both, the OECD Privacy Guidelines and the APEC Privacy Framework. Principle 15 contains a recommendation on international transfers of data, which endorses the use of contractual clauses for cross-border transfers of data for countries that do not provide an adequate level of protection pursuant to the principles and recommendations of the Madrid Resolution. The third paragraph provides exceptions for the transfer of data to States that do not provide the required level of protection, which might be raised where necessary and in the interests of the data subject in the framework of a contractual relationship, to protect the vital interests of the data subject or of another person or when legally required on important public interest grounds. The last paragraph of said principle establishes that applicable national legislation may grant powers on the supervisory authorities to authorize the international transfers falling within their jurisdiction before they are carried out and those conducting international transfers of data, should demonstrate and comply with the guarantees contained in the Resolution and in particular with the powers of supervisory authorities pursuant to their national legislation.

The Madrid Resolution is a non-binding instrument that aims to establish the grounds for an international treaty on data protection and transborder flows, however, so far the recommendations are used as a source of soft law that other countries could follow when enacting data protection legal frameworks.

---

[34] International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution) International Conference of Data Protection and Privacy Commissioners, 5 November 2009, available at:http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

5. EMERGING MECHANISMS FOR THE TRANSFER OF CROSS-BORDER DATA

As a result of the diversity of national legal regimes on data protection around the world, and in particular the global approaches on transborder data flows and the growth of cloud computing services, there are ongoing-efforts for companies based in Europe and in the Asia Pacific Region to help them comply with data transfers without the need of a third country to comply with the *"adequacy decision standard"* required by the European Commission. For example, in March 2014, Article 29 Working Party and the APEC Economies entered into a referential document that seeks to facilitate the compliance of personal data protection policies based on a certification system for companies operating both in the EU and APEC[35]. The certification forms part of the Cross-Border Privacy Rules (CBPR) of the APEC[36], which puts strong emphasis for companies in the implementation of the Accountability Principle[37] for the processing of personal data of their clients across the APEC member economies.

One of the current challenges is to make cross-border privacy rules and frameworks coexist and operate among the different legal systems across Europe and the Asia Pacific region, particularly for international transfers of data, an issue that in our view will not be easily achieved in the short term if Europe does not soften its strict and complicated rules on international transfers and improve the existent mechanisms to move and transfer data from the EU to other parts of the world.

---

35 See: Joint work between experts from the Article 29 Working Party and from APEC Economies on a referential for Requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents, available at:
http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

36 See *note* 33.

37 See *note* 32.

Regarding the issue of interoperability, paragraph 21 of the OECD Revised Privacy Guidelines expresses the general objective of Member countries to improve global interoperability of privacy frameworks through international arrangements that might offer practical effects to the OECD Privacy Guidelines. According to the OECD, *"there exists a range of approaches to interoperability among privacy frameworks. The US-EU Safe Harbour Framework, which was adopted under the EU adequacy regime and implemented in 2000, was an early example. Since then, several initiatives have been undertaken to bring together different approaches and systems of protection, including work by the privacy enforcement authorities within the framework of the EU Binding Corporate Rules and the APEC Cross-Border Privacy Rules System within the Asia-Pacific region"*[38].

Perhaps, one of the greatest challenges today in the field of data protection is to make all the legal frameworks —whether international, regional or national— work and operate properly without the enactment of barriers, restrictions and unnecessary regulatory bureaucracies particularly in the area of international data transfers, thus we strongly support that countries of the Asia-Pacific should give strong priority to make their national data protection frameworks work in a flexible and dynamic basis and allow data transfers from and to other countries as long as sufficient security safeguards have been established to protect the privacy of the information of data subjects and the respect of privacy as a fundamental human right.

---

[38] See Supplementary Explanatory Memorandum to the Revised OECD Privacy Guidelines, 2013, p. 33. For further information on interoperability between APEC's CBPR System and the European approach on cross-border transfers, see: Hunton & Williams, US. Chamber of Commerce, *"Business without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity"*, May 20014, pp. 26-27 available at: https://www.uschamber.com/sites/default/files/documents/files/021384_BusinessWOBorders_final.pdf.

6. THE STATUS IN LATIN-AMERICAN COUNTRIES WITH DATA PROTECTION LAWS

6.1. Countries of Latin America that have met the Adequacy Decision Standard

Since the entry in force of the EU Data Protection Directive in October 1998, only Argentina[39] and Uruguay[40] have met the *"adequacy decision standard"* of the European Commission in July 2003 and August 2012, respectively.

Argentina and Uruguay are two economies that are part of the MERCOSUR[41] area that historically have had strong ties with the European culture but not specially strong commercial relations with big economies like the United States, Canada and countries of the Asia-Pacific region. Argentina was one of the first countries that implemented a comprehensive data protection law and the

---

39 See: Commission Decision of 30 June 2003 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data in Argentina, published in the OJ L 168 on 05.07.2003, available at: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf

40 See: Commission Executive Decision C (2012) 5704 of 21 August 2012 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data in the Republic of Uruguay published in the OJ L 227/11 on 23.08.2012, available in Spanish at: http://privacyconference2012.org/wps/wcm/connect/4f619a804c810ce58f1fcf5ecf671ba0/Adecuacion_UE.pdf?MOD=AJPERES.

41 The Common Market of the South (MERCOSUR) was established in 1991 by the Treaty of Asuncion, which was later amended and updated by the Treaty of Ouro Preto in 1994. Mercosur is now a fully operative customs union conformed by Argentina, Brazil, Paraguay, Uruguay, Venezuela and Bolivia whose main purpose is to promote free trade, the exchange of goods and services, the free movement of people and the adoption of a common trade policy with other States, as well as with international and regional organizations. Bolivia, Chile, Colombia, Ecuador, Guyana, Peru and Suriname currently have associate member status. The website of Mercosur is available at: http://www.mercosur.int/

regulation of the habeas data in Latin America. When Argentina enacted its data protection law (*Ley No. 25,326*) in October 2000[42] —which regulates the processing of personal data contained in files, registries and databases pertaining to both, private and public entities— many countries in the region shared the view that they could follow the model adopted in Argentina.

Fortunately, this initial experiment in the region of trying to import and adopt the European data protection model had its pros and cons. On the one hand, it was very helpful for countries of the region to make them realize the urgent need to establish rules for the protection of the privacy of individuals in the processing of their personal data as a fundamental right, but on the other hand, the implementation of the European system in Argentina made many countries aware that the imported model had brought unintended administrative burdens and excessive bureaucracies for the supervisory authority as well as strict rules that very few companies and organizations —particularly small and medium sized companies— were willing to comply mainly due to the high costs involving compliance programs and specialized legal services.

Further, the early exercise of implementing data protection laws and in particular the adoption of the European model were extremely helpful for many countries in the region to carefully analyze and decide on the best approach to regulate data protection and transborder data flows at the national level. For example, Mexico gave priority to the protection of the right of access to information, transparency and data protection in the sphere of public entities and enacted legislation and rules for the protection of personal data in the public sector that have been in force since June 2003[43]. However, efforts to enact a data protection law

---

42 Argentina's Ley 25,326 de Protección de los Datos Personales is available at: http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

43 See VELASCO, Cristos, *"Transparency and Access to Government Information"* in "Cyber Law in Mexico", Part VIII, Wolters Kluwer Law & Business, 2013, pp. 337-344.

for the private sector took Mexico more than 10 years, precisely because one of the big issues —among others— in the drafting process was to achieve consensus in the regulation of transborder data flows, since Mexico had already adopted trade commitments with the United Sates and Canada trough the North American Free Trade Agreement (NAFTA) whose Chapter IX on Standard Related Measures prevent members countries from applying, or adopting standard measures that create unnecessary obstacles or barriers to trade and the free flow of information[44].

6.2. The Current Situation in other Latin-American Countries with Data Protection Laws

The approaches on the regulation of international transfers vary significantly among the countries of Latin America. In this section, we take a closer look at the provisions contained in the data protection laws and regulations of Mexico, Colombia, Peru and Costa Rica, countries that have enacted data protection legal frameworks in the last four years.

6.2.1. Mexico

The Federal Law on Protection of Personal Data in Possession of Private Parties (FLPPDPPP)[45] which is law that the regulates the

---

44 See NAFTA Article 904. 4. On 22 February 2008, the government representatives of the three NAFTA countries signed the *Statement on the Free Flow of Information and Trade in North America* in order to ensure that their regulatory regimes on privacy and data protection do not hinder cross-border data flows and international trade among them through the establishment of a trilateral committee that seeks to complement existing work in multilateral forums like the OECD and APEC. The *Statement on the Free Flow of Information and Trade in North America* is available at: http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/eng/gv00515.html

45 Ley Federal de Protección de Datos en posesión de los Particulares has been in force since 28 April 2010 and is available in Spanish at: http://protecciondatos.mx/wp-content/uploads/2011/06/LFPDPPP2.pdf

collection and processing of personal data by companies and private organizations contains a chapter that regulates national and international data transfers. Unlike most data protection laws in Latina America, Mexico's data protection law does not make any reference to the adequate level of protection that other countries should have for the processing of personal data.

Article 36 stipulates that when a data controller intends to transfer personal data to domestic and foreign parties other than the data processor, the data controller must provide them with the privacy notice and the purpose to which the data subject has limited the processing of his data. Said article provides that the processing shall be made pursuant to the privacy notice, which shall include a clause indicating whether the data subject agrees to the transfer of his data. Under this provision, the third party receiver will assume the same obligations as the data controller that has transferred the data.

The FLPPDPPP establishes exemptions for national and international transfers. Article 37 stipulates that domestic or international transfers of data may be carried out without the consent of the data owner in the following cases: (i) where the transfer is pursuant to a Law or Treaty to which Mexico is party; (ii) where the transfer is necessary for medical diagnosis or prevention, health care delivery, medical treatment or health services management; (iii) where the transfer is made to holding companies, subsidiaries or affiliates under common control of the data controller, or to a parent company or any company of the same group as the data controller, operating under the same internal processes and policies; (iv) where the transfer is necessary by virtue of a contract executed or to be executed in the interest of the data owner between the data controller and a third party; (v) where the transfer is necessary or legally required to safeguard the public interest or for the administration of justice; (vi) where the transfer is necessary for the recognition, exercise or defense of a right in a judicial proceeding, and (vii) where the transfer is necessary to maintain or fulfill a legal relationship between the data controller and the data subject.

The Regulation of the FLPPDPP contains a full chapter consisting of 10 articles where the conditions, obligations and the formalization for national and international data transfers are further specified. Article 70 regulates the transfers of personal data among holding companies, subsidiaries or affiliated of the data controller's group or responsible parent company through the use of internal data protection rules, the enforcement of which should be binding and as long as they comply with the FLPPDPP, its regulation and other applicable norms.

Regarding international data transfers, Article 75 allows the use of contractual clauses and other legal instruments which should contain at least the same obligations as those to which the data controller transferring personal data is subject, as well as the conditions under which the data subject consented to the processing of his personal data.

Article 76 of the Regulation allows data controllers —only when necessary— to request the opinion of the data protection agency IFAI as to whether an international transfer that they are carrying out complies with the FLPPDPPP and its Regulation. However, obtaining the opinion of the Mexico's data protection agency IFAI is only an option, but not necessarily a legal obligation that data controllers and entities exporting data should comply under the FLPPDPP.

6.2.2. Colombia

Colombia enacted a data protection law on 17 October 2012[46]. The law regulates the collection and processing of personal data registered in databases pertaining to both, the public and private sector.

---

[46] Ley Estatutuaria núm. 1581 del 17 de Octubre de 2012, por el cual se dictan disposiciones generales para la protección de datos personales, available in Spanish at: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

The conditions and exemptions for the transfer of data to other countries are set out in Article 26.

Paragraph first of Article 26 establishes as a general rule, the prohibition to transfer personal data to countries that do not provide an adequate level of protection. Such paragraph further establishes that a country might provide an adequate level of protection to personal data when the country in question complies with the standards established by the supervisory data protection agency, which is the *Superintendencia de Industria y Comercio*, and the level of data protection might not be lowered than the one required to data controllers pursuant to the law.

Article 26 also enlists six exemptions for data transfers, these are: (i) when the data subject has granted unequivocal and express authorization for the transfer; (ii) through the exchange of medical data when the processing is so required by data subjects or through public health reasons; (iii) securities and banking transfers pursuant to the respective legislation; (iv) agreed transfers contained in the sphere of international agreements that Colombia might be part of and based in the principle of reciprocity; (v) required transfers for the execution of a contract between the data subject and data controller or for the execution of pre contractual measures as long as the data subject authorizes them; (vi) legal transfers required for the safeguard of the public interest or for the acknowledgement, exercise or defense of a right in a judicial process. Said article contains two final provisions that stipulate that in cases where no exemption is provided for the transfer of personal data, the supervisory data protection agency might issue the corresponding statement regarding international transfers of personal data subject to the request of further information in order to comply with the possible scenarios required for its operation, and that the provisions contained in said article are applicable to personal data including data regulated under *Ley 1266 of 31 December*

2008[47] whose main purpose is to guarantee the constitutional right of individuals to know, amend or rectify their information contained in databases pertaining to the public administration or private entities and to guarantee the rights and liberties regarding the collection, processing and circulation of personal data pursuant to Article 15 of Colombia's Constitution.

Colombia's data protection law of October 2012 contains a provision on the use of Binding Corporate Rules, which stipulates that the national government shall enact its corresponding regulation for the certification of good practices on data protection and data transfers to third countries. Since the data protection law of 2012 has been in force for a short time, we are not in a position to assess precisely how the use of binding corporate rules is working in practice in this country.

According to Nelson Remolina, an academic expert on data protection in Colombia, *"Law 1,266 on Habeas Data and the Management of Personal Data of December 2008 does not contain adequate measures for international transfers of data mainly because the law grants the power to data exporters and not the data protection agency itself to decide if a third country provides an adequate level of protection for purpose of international transfers, which allows the flows of data without establishing sufficient legal safeguards for the protection of personal data of Colombian citizens"*[48].

---

47 Ley 1266 del 31 de Diciembre de 2008, que contiene disposiciones generales del Habeas Data y el manejo de datos personales is available at: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

48 Remolina Angarita, Nelson, *"¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estandar Europeo?"*, 16 International Law, Revista Colombiana de Derecho Internacional, 2010, pp. 517-520, available at: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Tiene-Colombia-nivel-adecuado….Nelson-Remolina1.pdf It is worth mentioning that Remolina's article was written previous to the enactment of Ley Estatutuaria núm. 1581 from 17 October 2012. After the exchange of communications with him, the Colombian author is of the opinion that Colombia might now have the minimum requirements to comply with the adequacy decision model of the European Commission.

6.2.3. Peru

The President of Peru enacted Law No. 29,733 on Protection of Personal Data on June 2011[49]. Said law regulates the collection and processing of data contained or to be destined in databases pertaining to both, the public and private administration when the processing is conducted in national territory.

The law contains a definition and two provisions governing transboundary data flows. The definition of transboundary data flows is contained in Art. 2(8) and it is defined as follows: *"international transfer of personal data to a destinatary located in a country other than the country of origin of personal data, regardless of the support which they are found, the means used for the transfer and the processing granted".*

Article 11 of the law stipulates as a general principle for the flows of personal data that a sufficient level of protection of personal data shall be afforded in order for data to be processed, or at least equivalent to the measures contained in the law or the international standards on the subject.

Article 15 sets out the conditions and exemptions to the flows of personal data. The first paragraph establishes a general rule that both, data subjects and data controllers are permitted to carry out transfers of personal data only if the country of destination maintains an adequate level of protection pursuant to the legislation. The second paragraph stipulates that when a country does not provide an adequate level of protection, the party carrying out transborder flows of personal data shall guarantee that the processing of personal data is made pursuant to the provisions of the law.

The last paragraph of Article 15 enlists eight exemptions to comply with the second paragraph, which are: (i) international agreements on the subject matter where Peru is a party; (ii)

---

[49] Ley núm. 29733 de Protección de Datos Personales was published on 21 June 2011 is available at: http://www.claro.com.pe/portal/recursos/pe/pdf/Ley29733.pdf.

international judicial cooperation; (iii) international cooperation between intelligence organizations in the fight against terrorism, drug and human trafficking, money laundry, corruption and other forms of organized crime; (iv) when data are necessary for the execution of a contractual relation where the data subject is a party including activities related to user authentication, service and improvement support, monitoring of the quality service, support for the account's billing and those activities required for the management of any contractual relation; (v) when dealing with banking and securities transfers and pursuant to the applicable law; (vi) when the flow of personal data is conducted for the protection, prevention, diagnosis or medical or surgery treatment of the data subject or when it is necessary for epidemiology studies or analogous as long as adequate disassociation procedures are applied; (vii) when the data subject has given previously his informed, expressed and unequivocal consent; (viii) others as established in the regulation of the law and subject to the data protection principles provided in Article 12 of the law.

In addition, the Regulation of the Law on Protection of Personal Data[50] contains a full chapter (Arts. 18-26) on transfers of personal data that establishes: (i) a definition on transborder data flows and the obligation of the parties transferring personal data to comply with the provisions of the law and the regulation[51]; (ii) the obtaining of consent of the data subject, except for the exceptions listed in Art. 14 of the law and limited exclusively for the purpose that justifies its transfer[52]; (iii) to prove that the transfer was conducted pursuant to the law and the regulation, having the data controller always the burden of proof[53]; (iv) in case of transfers

---

50 Reglamento de la Ley núm. 29733 de Protección de Datos Personales was published on 22 March 2013 and is available at: http://www.minjus.gob.pe/wp-content/uploads/2013/04/DS-3-2013-JUS.REGLAMENTO.LPDP_.pdf

51 Regulation Article 18.

52 Regulation Article 19.

53 Regulation Article 20.

of personal data to a company group, subsidiaries or affiliates processing data, said companies will need to have a code of conduct establishing internal rules on the protection of personal data pursuant to Article 31 and should be duly registered before the data protection agency[54]; (v) the establishment of formal mechanisms that could show that the owner of databases communicated data controllers the conditions and the consent of data subjects for the processing of personal information[55]; (vi) the possibility of conducting transborder data flows when both, the importing or reception party assume the same obligations pertaining to owners of databases or the responsible or exporting parties transferring personal data[56].

Article 25 sets out the conditions for the use of contractual clauses or other legal instruments between data controllers and the exporter of data where at least, the same conditions should be established as well as those conditions where the data subject consented to the processing of his data.

Article 26 allows the owners of databases or those parties responsible for the processing of data to request the opinion of the General Direction of Personal Data Protection on whether the conditions on transborder data flows are fulfilled pursuant to the law and the regulation. The last paragraph of this article establishes the obligation to acknowledge the General Direction of Personal Data Protection any information regarding transborder data flows.

6.3.4. Costa Rica

The *Law on Protection of Individuals for the Processing of Personal Data of September 2001*[57] regulates the processing of personal data of automatized and manual databases pertaining to both, public

---

54 Regulation Article 21.

55 Regulation Article 23.

56 Regulation Article 24.

57 Ley núm. 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales was published in September 5, 2001.

and private organizations and any modality of the subsequent use of such data.

Article 14 establishes as a general rule that the parties responsible for the use of databases both, public or private might only be able to transfer data contained therein when the data subject has expressly and legally authorized such transfer and the transfer is conducted according to the principles and rights set out in the laws of that country.

The *Regulation of the Law on Protection of Individuals for the Processing of Personal Data of March 2013*[58] contains a chapter on the transfer of personal data consisting of four articles that set out the conditions for the transfers, the compliance of minimum acting protocols, the burden of proof of the data controller and the use of contracts for the transfer of personal data setting out specific obligations for data controllers for the transfer of data.

Neither the law nor the data protection regulation makes any particular reference to international transfers of data to third countries or to the term *"adequate level of protection"*.

7. CONCLUSIONS

The adequacy decision standard contained in the Data Protection Regulation Proposal of the European Commission is a mere extension of the rules contained in the EU Data Protection Directive of 1995 that when enter into force will continue to set restrictions for international transfers of data to third countries that do not provide the adequate level of protection required by the European Commission and the opinion of the European Data Protection Board that will assume the role and activities of Article 29 Working Party.

---

58 Reglamento de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales. Decreto Ejecutivo núm. 37554-JP of 5 March 2013.

The adequacy decision model of the European Commission contained in its Data Protection Regulation Proposal is in our view, an obsolete model that has proved to be unsuccessful with regards to international transfers to third countries. The Data Protection Regulation proposal currently puts a strong emphasis in the use of binding corporate rules and standard contractual clauses for the transfer of personal data to countries that do not provide the required *"adequate level of protection"*. Nevertheless, the approval of such instruments is subject to the opinion of the supervisory authority of the country exporting the data and the internal procedural mechanisms of the European Commission, which will mean further barriers and bureaucracies for companies and organizations established in countries that do not have the adequate level of protection and that want to export data to companies or organizations based in Europe as part of their usual business activities.

Emerging regional certification mechanisms like APEC's CBPR system —which aim to help companies located in the Asia-Pacific region to comply with data transfers without the need of having the European Commission *"adequacy level of protection"* in place— have the potential to offer flexibility and legal certainty to exports of data to companies and organizations located in the Europe and Asia trough the mutual acknowledgement of the required safeguard measures contained in the Data Protection Regulation Proposal. However, it remains to be seen in the coming years whether the safeguards and certification programs established under both systems could smoothly interoperate without the need of establishing unnecessary procedures and bureaucracies for companies and organization operating in both regions.

The challenges remain undoubtedly at the national level and especially in countries of Latin America where the approaches to international transfers of data are not uniform and consistent with the *"adequacy decision model"* of the EU as previously analyzed in this article. We are of the opinion that the European Commission should soften the rules and procedures for the use of safeguards instruments like standard contractual clauses and binding

corporate rules to export data to other countries and simplify the verification procedures and should fully abolish the mechanism of declaring that third countries have met the adequacy level of protection.

Countries like Colombia and Peru establish specific rules for international data transfers to countries that provide and adequate level of protection largely based on the language of the EU Data Protection Directive of 1995, but paradoxically the data protection laws and regulations of both countries have not yet met the *"adequacy level of protection"* of the European Commission. Said data protection laws and regulations also provide the possibility for data controllers and data processor to use standard contractual clauses and contractual arrangements for international data transfers and this is clearly a window of opportunity not only to promote the use of such safeguards with European based companies but also with companies based in other regional commercial blocks like the Asia-Pacific, where Peru, Mexico and Chile are members.

Mexico is perhaps the only country of the region that strikes a fairly good balance in its data protection law and regulation regarding the content of the rules on international data transfers where there is no specific mention on the *"adequate level of protection"*. Like Colombia and Peru's, Mexico's legislation offers the alternative for the use of standard contractual clauses and other legal instruments for international transfer of data that unfortunately have not been yet been fully implemented at the practical level. The use of such instruments are likely to get further developed and acceptance considering the recent adoption of Mexico of APEC's Cross-Border Privacy Rules.

There is clearly relevant work to be done in Latin America with regards to the promotion and use of safeguards for international data transfers and in particular the use of binding corporate rules and standard contractual clauses among the business community in order to comply with the standards for international data transfers contained in Europe and the Asia-Pacific, an area that data

controllers, data processors and specially data protection authorities in the region should closely focus their attention.

Finally, we'd like to conclude this article by urging the European Commission to abolish the use of the "*adequacy level of protection*" mechanism in countries of Latin America based not only on the experience and poor results obtained so far with other countries but particularly by taking into account the differences of the current legal approaches to international data transfers in the region. The European Commission and European data protection authorities should instead focus their attention in improving the safeguard mechanisms for the transfers of personal data to countries of Latin America and cooperate with data protection authorities to make such safeguards compatible with the legal tradition and culture of countries of Latin America in order to allow the flow of international data transfers on a flexible basis and avoid the possibility of trade disputes and tensions at the regional and international level.

8. BIBLIOGRAPHY

8.1. Books and Chapters

RUDGARD, Sian, *"Origin and Historical Context of Data Protection Law"* in *European Privacy. Law and Practice for Data Protection Professionals*, International Association of Privacy Professionals (IAPP), Chapter One, 2012.

USTARAN, Eduardo, *"International Data Transfers"* in *European Privacy. Law and Practice for Data Protection Professionals*, International Association of Privacy Professionals (IAPP), Chapter Twelve, 2012.

VELASCO, Cristos, *"Transparency and Access to Government Information"* in *Cyber Law in Mexico*, Part VIII, Wolters Kluwer Law & Business, 2013.

8.2. Articles and Reports

BENNET, Colin and Charles Raab, "*The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response*" The Information Society. An International Journal, Volume 3, Issue 3, 1997.

CUIJPERS, Colette, PURTOVA, N. & KOSTA E., *"Data Protection Reform and the Internet: The Draft Data Protection Regulation"*. Tilburg Law School Legal Studies Research Paper Series No. 03/2014 a.

GREENLEAF, Graham, *"The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108?"* University of Edinburgh School of Law, Research Paper Series No. 2012/12.

Hunton & Williams, US. Chamber of Commerce, *"Business without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity"*, May 20014.

KUNER, Christopher, *"Developing an Adequate Legal Framework for International Data Transfers"* Springer Science + Business Media B.V. 2009.

KUNER, Christopher, *"Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future"*, OECD Digital Economy Paper, No. 187 OECD publishing 2011.

POULLET, Yves, *"Transborder Data Flows and Extraterritoriality: The European Union Position"*, CRID March 21, 2007.

REMOLINA Angarita, Nelson, *"¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estandar Europeo?"*, 16 International Law, Revista Colombiana de Derecho Internacional, 2010.

SULLIVAN, Clare, *"Protecting digital identity in the cloud: Regulating cross-border data disclosure"*. Computer Law and Security Review (30), 2014.

8.3. International Guidelines and Recommendations

APEC Privacy Framework.

APEC Cross-Border Privacy Rules System. Policies, Rules and Guidelines.

International Standards on the Protection of Personal Data and Privacy (*The Madrid Resolution*) 5 November 2009.

Joint work between experts from the Article 29 Working Party and from APEC Economies on a referential for Requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980.

Recommendation of the OECD Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C(80)58/FINAL as amended on 11 July 2013 by C(2013)79].

Explanatory Memorandum to the Revised OECD Privacy Guidelines, 2013.

United Nations Guidelines for the Regulation of Computerized Personal Data Files adopted by the UN General Assembly Resolution 45/95 of 14 December 1990.

North American Free Trade Agreement (NAFTA).

Statement on the Free Flow of Information and Trade in North America of 22 February 2008.

8.4. European Legislation and Official Documents of European Institutions

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (*Convention 108*).

Additional Protocol to Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Supervisory Authorities and Transborder Data Flows.

Directive 95/46 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 of the free movement of such data published in the Official Journal of the European Union No. 281 of 23/11/1995.

Regulation EU 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.

Proposal for a Regulation 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 COM (2012) 11 final of 25 January 2012 (General Data Protection Regulation).

Commission Decision of 30 June 2003 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data in Argentina, published in the OJ L 168 on 05.07.2003.

Commission Executive Decision C (2012) 5704 of 21 August 2012 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data in the Republic of Uruguay published in the OJ L 227/11 on 23.08.2012.

Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, "*First orientations on Transfer of Personal Data to Third Countries. Possible Ways Forward in Assessing Adequacy*". Discussion Document adopted by the Working Party on 26 June 1997.

Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *"Transfers of personal data to third countries: Applying Article 25 and 26 of the EU data protection directive"*. Working document adopted by the Working Party on 24 July 1998.

European Commission Memo: *"Data Protection Day 2014: Full Speed on Data Protection Reform"*, Brussels, MEMO/ 14/60 of 27 January 2014.

European Commission Memo: *"Progress on EU data protection reform now irreversible following European Parliament vote*", Brussels MEMO/14/186 of 12 March 2014.

Article 29 Data Protection Working Party Rules of Procedure of 15 February 2010.

Commission Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, Official Journal of the EU/Legislation (OJL) 181/19 of 4 July 2001.

Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, Official Journal of the EU/Legislation (OJL) 385/74 of 29 December 2004.

8.5. Latin-American Legislation

Argentina

Ley 25,326 de Protección de los Datos Personales.

Colombia

Ley Estatutuaria No. 1581 del 17 de Octubre de 2012, por el cual se dictan disposiciones generales para la protección de datos personales.

Ley 1266 del 31 de Diciembre de 2008, que contiene disposiciones generales del Habeas Data y el manejo de datos personales.

Costa Rica

Ley No. 8968 de Protección de la Persona Frente al Tratamiento de sus Datos Personales

Reglamento de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales. Decreto Ejecutivo No. 37554-JP

México

Ley Federal de Protección de Datos en posesión de Particulares

Reglamento de la Ley Federal de Protección de Datos en posesión de Particulares

Perú

Ley No. 29733 de Protección de Datos Personales

Reglamento de la Ley No. 29733 de Protección de Datos Personales

8.6. Websites

Article 29 Working Party http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

Asia-Pacific Economic Cooperation Forum (APEC) http://www.apec.org

Bogota Jurídica Digital http://www.alcaldiabogota.gov.co/

Claro.Com Perú http://www.claro.com.pe/wps/portal/pe/sc/personas

Council of Europe http://www.coe.int

European Commission http://ec.europa.eu/index_en.htm

European Union http://europa.eu/

31st International Conference of Data Protection and Privacy Commissioners, Madrid, Spain 4-6 November 2009 http://www.privacyconference2009.org

34a Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Punta del Este Uruguay 23-24 October 2012 http://privacyconference2012.org/

Industry Canada http://www.ic.gc.ca/eic/site/icgc.nsf/eng/home

Información Legislativa y Documental del Ministerio de Economía y Finanzas Públicas de Argentina http://www.infoleg.gov.ar/

Mercosur http://www.mercosur.int/

Ministerio de Justicia y Derechos Humanos de Perú http://www.minjus.gob.pe/

Official Journal of the European Union http://eur-lex.europa.eu/oj/direct-access.html

Organization for Economic Cooperation and Development (OECD) http://www.oecd.org/

Protección Datos México (ProtDataMx) http://protecciondatos.mx

Social Science Research Network (SSRN) http://www.ssrn.com/en/

United Nations High Commission for Refugees (UNHCR) http://www.refworld.org/

US Chamber of Commerce https://www.uschamber.com/