International Data Transfers and Data Protection Legislation: Challenges and Opportunities for Brazilian Trade

Dr Christian Perrone
Institute for Technology and Society of Rio de Janeiro
Rio de Janeiro, Brazil
c.perrone@itsrio.org

Amy Ertan
Royal Holloway, University of London
London, United Kingdom
amy.ertan.2017@rhul.ac.uk

Abstract

On 26h June 2019, after 20 years of negotiations, the European Union and MERCOSUR - a South American trading partnership involving Brazil, Argentina, Uruguay and Paraguay[1] - signed a historic trade agreement[2]. While some ratification challenges may be expected[3], it is accepted that successful implementation of the pact promises to open up economic trading markets significantly for products and services for all parties. This increased flow of trade and services generates an additional need for effective facilitation of the free flow of data, a requirement that is heavily dependent on regional and national data protection regulation.

The most influential of these regulations is the European Union's General Data Protection Regulation (GDPR). Effective as of March 2018, GDPR establishes standards for data protection and privacy for all citizens within the European Union and the EEA[4]. MERCOSUR does not currently have an equivalent regulatory framework, however Argentina and Uruguay have implemented comprehensive national data protection legislation, and the Brazilian Data Protection Regulation (*Lei Geral de Proteção de Dados*, or LGPD) enters into force as of August 2020.[5]

---

[1] Venezuela is also a member of MERCOSUR, yet following democratic unrest, the country has been suspended since 2016.

[2] European Commission- MERCOSUR announcement (9 July 2019) http://ec.europa.eu/trade/policy/countries-and-regions/regions/mercosur/ <Accessed 1 August 2019>

[3] Austria rejects EU-Mercosur trade deal over Amazon fires https://www.theguardian.com/world/2019/sep/19/austria-rejects-eu-mercosur-trade-deal-over-amazon-fires <Accessed 21 September 2019>

[4] Note: European Economic Area. For more information please see: https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:European_Economic_Area_(EEA)

[5] Paraguay does not have a comprehensive data protection legislation. However, as of this year there as discussion on a specific bill to regulate the matter: *Proyecto de Ley "De Protección de datos personales".* Available in Spanish at: http://silpy.congreso.gov.py/expediente/115707 <Accessed 2 August 2019>.

This article examines the implications of facilitating data transfer mechanisms that are compliant with data protection regulation, considering the challenges for Brazil as both importers and exporters of data. The regulatory landscape includes the LGPD, the incoming Brazilian Data Protection Authority, existing international requirements due to GDPR and the considerations of MERCOSUR and additional trade agreements. *The article will walk through two use-cases where Brazil is both the 'importer' and 'exporter' of data, highlighting potential distinctions which may differ depending on counterparts' relative data protection regulation.* The article will also consider the practical challenges in securely implementing these legislative pieces and highlights the guidance that will be required to promote effective organisational adherence.

Full Paper

On 26h June 2019, after 20 years of negotiations, the European Union and MERCOSUR - a South American trading partnership involving Brazil, Argentina, Uruguay and Paraguay[6] - signed a historic trade agreement[7]. While some ratification challenges may be expected[8], it is accepted that successful implementation of the pact promises to open up economic trading markets significantly for products and services for all parties. This increased flow of trade and services generates an additional need for an effective facilitation for the free flow of data, a requirement that is heavily dependent on regional and national data protection regulation.

The most influential of these regulations is the European Union's General Data Protection Regulation (GDPR). Effective as of March 2018, GDPR establishes standards for data protection and privacy for all citizens within the European Union and the EEA[9]. MERCOSUR does not currently have an equivalent regulatory framework, however Argentina and Uruguay have implemented comprehensive national data protection legislation, and Brazil approved in 2018 the

[6] Venezuela is also a member of MERCOSUR, yet following democratic unrest, the country has been suspended since 2016.

[7] European Commission- MERCOSUR announcement (9 July 2019) http://ec.europa.eu/trade/policy/countries-and-regions/regions/mercosur/ <Accessed 1 August 2019>

[8] Austria rejects EU-Mercosur trade deal over Amazon fires https://www.theguardian.com/world/2019/sep/19/austria-rejects-eu-mercosur-trade-deal-over-amazon-fires <Accessed 21 September 2019>

[9] Note: European Economic Area. For more information please see: https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:European_Economic_Area_(EEA)

General Data Protection Legislation (*Lei Geral de Proteção de Dados*, or "LGPD")[10][11].

This article examines the implications of facilitating data transfer mechanisms that are compliant with data protection regulation, considering the challenges for Brazil as both importers and exporters of data. The regulatory landscape includes the LGPD, the incoming Brazilian Data Protection Authority, existing international requirements due to GDPR and the considerations of MERCOSUR and additional trade agreements. The article will also consider the practical challenges in securely implementing these legislative pieces and highlights the guidance that will be required to promote effective organisational adherence.

1. Brazilian Data Protection Regulation (LGPD) and Territorial Scope

LGPD holds major implications for organisations that transfer personal data to other jurisdictions[12]. With inspiration drawn from the European Union's General Data Protection Regulation (GDPR), a key part of the LGPD addresses the topic of cross-border jurisdiction. As with GDPR's extraterritorial powers[13], LGPD confirms its applicability not only to organisations processing personal data processed within Brazil, but also to the processing of Brazilian citizens' personal data in other jurisdictions[14].

GDPR is premised on the idea that the physical location of personal data should not determine the standard of protection guaranteed to the data subject. The logic is that personal data should be involved by a so called "bubble of protection" wrapping the data in all the safeguards present

[10] The Brazilian Data Protection Legislation is not yet into force. It is set to enter into force as of August 2020, yet, there are several bills in Congress postponing the entry into force of LGPD wither its entirety or of certain parts, particularly the capacity of the DPA to issue sanctions. For a partial picture see: https://iapp.org/news/a/brazilian-senate-postpones-its-national-data-protection-law/. Recently, the President issued a decree postponing LGDP as well, but it is dependent on approval of Congress. For an analysis of the whole entanglement in Portuguese, see: https://tecfront.blogosfera.uol.com.br/2020/04/30/mp-de-bolsonaro-atrasa-a-entrada-em-vigor-da-lei-de-protecao-de-dados/. <Accessed 4 May 2020>.

[11] Paraguay does not have a comprehensive data protection legislation. However, as of this year there as discussion on a specific bill to regulate the matter: *Proyecto de Ley "De Protección de datos personales".* Available in Spanish at: http://silpy.congreso.gov.py/expediente/115707 <Accessed 2 August 2019>.

[12] DLA Piper, Data Protection Laws of the World, Brazil. Available at: https://www.dlapiperdataprotection.com/index.html?t=transfer&c=BR

[13] GDPR has extra-territorial applicability - which means the legislation applies to all organisations processing the personal data of EU citizens, regardless of the organisation's location. It therefore also applies to non-EU entities. For more information please see GDPR's Article 3 on territorial scope: SVANTESSON, Jan. *Art. 3 - Territorial Scope. In.:* Commentary on the EU General Data Protection Regulation (GDPR), upcoming, p. 6. Available at: https://works.bepress.com/christopher-kuner/1/.

[14] ONE Trust, What is Brazil General Data Protection Law, LGPD. Available at: https://www.onetrust.com/what-is-the-brazil-general-data-protection-law-lgpd/

in their original legal system. This "bubble" either remains when data crosses jurisdictional borders or is substituted by another based on adequate similar standards of protection.[15] Art. 3, LGPD, in consonance with the Brazilian Internet Bill of Rights (*Marco Civil da Internet, Lei 12.965/14*), mirrors such regulation. The Brazilian regulation is applicable no matter the means employed or where data is located or even where the company has its headquarters. What is relevant is (i) whether the processing operation is carried out in the country; the data collection is done within the territory; or (ii) the purpose of the processing activity is to target (offer goods, services) to, or (iii) based on data of individuals located in the national territory. Hence, GDPR and LGPD extend their territorial scope beyond their borders. Transfers, when allowed, need to be kept under strict guarantees.

2. Conditions for Cross-Border Data Transfers

GDPR and LGPD outline their respective approaches to cross-border data transfers, in which transfers of data to third-party countries may only take place subject to certain conditions on the part of both the data exporter and importer.[16] International transfers, then, should not be seen as exceptions nor be restricted. They should, however, be controlled and based on an exhaustive list of conditions delineated at the respective legislations.

As a preliminary note, it is important to bear in mind that neither system consider all movement of data that crosses borders as international transfers where safeguards apply. When someone, for instance, accesses personal data on a website in a different state, this transfer is not covered by data protection legislation.[17] As for transfers that are covered, the regulations create two categories of receiving countries: countries considered safe (adequate),[18] and the ones not at first

[15] One should bear in mind that data protection is understood expressly as a human right within the European System. It stands to reason that its obligations would aim at protection rights further than the specific geographical scope of the EU. (KUNNER, Christopher. *Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law*. *In.:* 5(4) IDPL (2015), pp. 242, 243. Available at: https://doi.org/10.1093/idpl/ipv019.

[16] From initial conception the intention was to align the Brazilian cross-border transfers with GDPR standards on the matter. (*Parecer da Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei* . Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1664233&filename=PEP+2+PL406012+%3D%3E+PL+4060/2012 <Accessed 1 August 2019>)

[17] Otherwise, much online activity would not be possible or considered illegal.

[18] To identify an adequate country, there should "a detailed evaluation of the legal system of the country to which the data are to be transferred". This means an analysis of the compatibility of data protection system the receiving country has. (KUNER, Christopher. *Article 46: Transfers subject to appropriate*

blush safe (not adequate). For the latter, safeguards do apply,[19] unless in exceptional circumstances provided in the legislation.

GDPR specifies the conditions under which a valid transfer may occur. The valid mechanisms include use of adequacy rulings,[20] additional appropriate safeguards (such as binding corporate rules or contractual clauses[21]) or, for exceptional circumstances,[22] on a case-by-case basis[23]. The language within LGPD is similar in terms of restrictions - with confirmation that cross-border data transfers are permissible through either a use of an equivalence - adequacy threshold which the third party countries must meet (similar to GDPR and the adequacy decisions mechanism)[24], or through the use of contractual mechanisms and contractual clauses as approved by the DPA. LGPD also allows for transfer in exceptional circumstances, which are similar in nature to the outlined GDPR limitations.[25]

These similarities are advantageous in three ways. First, by choosing similar requirements to the EU regulation, Brazil is able to adopt an approach that has already shown applicability and success in practice, reducing the chances of unpredictable consequences. Second, for the Brazilian organizations already complying with GDPR through the use of contractual clauses, it is likely fewer burdensome changes will be required, and the complications associated with compliance with multiple international regulations are minimised. Finally, the Brazilian similarities

safeguards. In.: Commentary on the EU General Data Protection Regulation (GDPR), upcoming, p. 6. Available at: https://works.bepress.com/christopher-kuner/1/.)

[19] The mentioned safeguards are meant to establish a specific regime so that transfers that cross-jurisdictional borders themselves become protected - in a similar fashion to the sending State - despite the legal regime in place in the receiving country.

[20] GDPR, art. 45. Transfers on the basis of an adequacy decision: A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

[21] Contractual Clauses must be either standard contractual clauses adopted by the Commission or adopted by a supervisory authority and approved by the Commission, or private clauses subject to the authorisation from the competent supervisory authority.

[22] Exceptional circumstances such as the following: explicit consent to the proposed transfer, the transfer is necessary for the performance of a contract between the data subject and the controller, transfer is necessary for important reasons of public interest; defence of legal claims; protect the vital interests of the data subject or of other persons; or made from a register under certain specific conditions. (Art. 49, GDPR).

[23] Fox Rothchild LLP, *Cross-Border Transfers of Personal Data in Light of GDPR.* https://dataprivacy.foxrothschild.com/2018/03/articles/european-union/gdpr/cross-border-transfers-of-personal-data-in-light-of-gdpr/ <Accessed 1 August 2019>

[24] LGPD, art. 34 establishes that the Brazilian Data Protection authority will establish

[25] LGPD, art. 33.

demonstrate an allied - and high - data protection approach to the GDPR and this may assist in paving the way to Brazil achieving adequacy status and ease data transfers with the EU (see below for further analysis).

In practice

In the case of importing or exporting activities, the proper treatment of personal data becomes paramount for compliance with relevant regulations.

A. Case study: Brazil as exporter of data (sending State)

Organisations who wish to transfer personal data outside of Brazil's jurisdiction must comply with LGPD requirements. As a first step, any data processing (including for transfer) must have an appropriate legal basis as *per* art. 7, LGPD. As a further step, it should be determined whether the receiving country is considered adequate by the Brazilian Data Protection Authority.[26] If it is, then the transfer can occur. If not, then, it can only go through under one of the valid safeguarding mechanisms available within LGPD.[27] This means that any company sending personal data overseas can only do so under the protection of an agreement that guarantees the respect of the Brazilian standards of protection. This can be achieved through binding corporate rules, specific contractual clauses - accepted or established by the Brazilian DPA, or certification mechanisms - accented prior by the Brazilian DPA.

Example: Consider a Brazilian tourism agency that is booking hotels in different countries in the world. The agency has to transfer personal data in order to finalize the bookings, has to send at least the persons' names. Considering Brazil's DPA has not yet released a list of third-party countries that are deemed to provide an adequate level of data protection to allow data transfer without additional mechanisms, this agency will have to rely on contractual clauses with its partners that guarantee the level of protection required within the LGPD. This is a relatively cumbersome mechanism; the company would have to negotiate with its various vendors and would have had the need to secure the authorization from the client (consumer) in order to transfer internationally the data.

[26] LGPD, art. 33, I and 34.
[27] LGPD, art. 33, II.

B. Case study: Brazil as importer of data (Receiving State)

The situation does not change dramatically considering Brazil as an importer of data. One can flip the situation around and the agency now is Europe and is booking a hotel for its client in Brazil. The company here, the hotel, has to process the information in order to secure the service. It needs the personal data from the client of the European tourism agency. Since Brazil is not in the list of adequate countries, in order for the personal data from the client to be transferred, they must have an agreement that guarantees the European standard of protection within Brazil.
LGPD art. 3 § 2º coupled with art. 4, IV considers the aforementioned circumstances. It makes Brazil open to receiving and processing data coming from other jurisdictions. It allows for the processing in Brazil in accordance with the standards provided in such agreements. However, the process is as assumed, a cumbersome one. There has to be such safeguard mechanisms in place.

In the context of international trade, the idea of adequacy can be of a central consideration and goal for Brazil. Upon achieving adequate status, despite being a country outside the E, it will be able to receive personal data without any additional safeguards deemed necessary.[28] GDPR's Article 45[29] on *Transfers on the Basis of an Adequacy Decision* outlines the mechanisms of Adequacy Decisions, and on what basis the European Commission assesses the adequacy of the level of protection provided by the jurisdiction in question. These include a consideration of the rule of law, and regulation displaying respect for human rights and fundamental freedoms, existing commitments the state has made with respect to data protection, and the functioning of an independent data protection authority.

Should Brazil achieve an adequacy decision from the European Commission, or align same adequacy requirements in LGPD, then, fewer contractual clauses would be needed to satisfy regulatory transfer mechanisms. This is a favourable path for trade agreements, for example. The agreement between MERCOSUR and the EU would be facilitated and further trade would be unimpeded. Implementation, however, must be genuine - to achieve adequacy, a number of

[28] Adequacy decisions - How the EU determines if a non-EU country has an adequate level of data protection.https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[29] EUR-LEX - Access to European Union Law - Document 32016R0679 - EN: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

relevant safeguards apply. Compliance with LGPD will often require an improved approach to information security, relating specifically to the storage and protection of personal data.

Example 1: A Brazilian software organisation wishes to enter a contract with a French healthcare firm, which would require the processing of the personal data of French citizens. As Brazil is not on the EU list of 'Adequate States'[30]*, a contractual clause and/or appropriate safeguards must be agreed by both parties and approved by the French.

Adequacy Decisions and Brazil

Within Latin America, Uruguay and Argentina have been recognised by the European Commission as jurisdictions providing adequate data protection.[3132] For Brazil, achieving an adequacy decision would be an important step in facilitating international data transfers across the EU and EEA, and possibly with other countries deemed adequate.[33]

We can compare Brazil's regulatory stance against Uruguay to assess possible Brazilian futures. Uruguay, as well as holding adequacy status, has a DPA that is very similar in structure to the Brazilian Data Protection Authority as it stands.[34] They are both administrative organs which have technical independency, without having a separate legal personality. This was not seen as an insurmountable obstacle for the EU to recognize the Uruguayan DPA as compatible to the tenets of data European data protection regime and considered the country as adequate.[35]

---

[30] There are 12 "adequate states"- Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay - and the United States under Privacy Shield. For further detail please see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en <Accessed 1 August 2019>

[31] There are 12 "adequate states"- Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay - and the United States under Privacy Shield. For further detail please see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en <Accessed 1 August 2019>

[32] For a reflection on Argentina's adequacy status judgement, please see https://www.itnation.lu/eu-and-mercosur-strike-first-trade-agreement-a-tech-and-data-protection-perspective/ <Accessed 1 August 2019>

[33] Considering how similar the criteria between the two pieces of legislation (GDPR and LGPD), there is a reasonable expectation that the Brazilian data protection authority will align its adequacy list with that of the European Commission.

[34] PARENTONI, Leonardo. Autoridade Nacional de Proteção de Dados brasileira: uma visão otimista. *In.:* Revista do Advogado, São Paulo, 2019.

[35] A comparative study may be found at: ITS Report, "Transferência de dados entre Brasil, União Europeia e Reino Unido: Análise do Processo de Adequação", 2019. Available at: https://itsrio.org/pt/publicacoes/transferencia-de-dados-entre-europa-brasil/.

The same happened for the Argentinian DPA. It is more akin the European standards and was recognized as compatible. Brazil should follow suit. Considering them together, an opportunity is created for the whole MERCOSUR to be adequate, three out of four countries[36] would be considered adequate, having close to 260 Million people covered by similar standards of protection. Such efforts are sure to facilitate trade not only between countries in the EU and the three countries in MERCOSUR but also create an area of free flow of data. This is sure to boost economic activity amongst participants and will also provide an added incentive for Paraguay (the fourth member) to initiate the process to raise its standards of data protection to be in sync with its neighbours and partners. A final note to add is that MERCOSUR countries could mutually recognize themselves as adequate within their own system which would establish a net of adequate countries where personal data can flow.

Complying with Data Transfer & Secure Storage/ Processing in practice

Implementing data protection regulation is no easy feat, but it is required. Weaknesses in data protection have occurred to the detriment of millions of citizens - in 2018, an InfoArmour report[37] uncovered that over half (57%) of Brazil's citizens had their social security numbers ('CPFs') exposed online through a publicly accessible directory. Should a similar breach occur after LGPD is fully implemented, the organisation would expect the DPA to enforce some sort of punitive action. Additionally, as well as the principle-based obligations to protect customer data, compliance requires a significant amount of attention on ensuring the secure processing and storage of personal data. This may be difficult to implement in practice, and GDPR requirements prompted widespread operational changes across organisational practice globally.

The cost of compliance with data transfer requirements (and wider adherence) is highly likely to be disproportionately difficult for small-medium enterprises. Large multinational firms have the benefit of greater resources to spend on legal and operational efforts to comply, while many will already be compliant with GDPR (Google, Facebook, Itaú Unibanco, Petrobras), therefore having fewer tasks to complete to reach the data protection standards required by LGPD. The similar

[36] For the purpose of this article, Venezuela that is still suspended from MERCOSUR will not be considered as a full member due to its current status.
[37] InfoArmor reports identification numbers of 120 million Brazilians exposed online: https://cdn2.hubspot.net/hubfs/3836852/PCOs/InfoArmor_Brazilian%20Exposure%20Report.pdf <Accessed 28th July 2019>

burden was highlighted and attended to (with varying effect) within the process of GDPR implementation. ENISA, the European Union Agency for Cyber Security, released guidelines for SMEs on the security of personal data processing[38] while the European Commission has guidance designed for non-experts, using clear language to explain the actions small businesses must take to achieve GDPR compliance[39]. Nonetheless, LDPD will require action from - and place pressure on - SMEs to guarantee the security and integrity of their data. With Sebrae reporting that 99% of Brazilian businesses fall into the 'SME' category, and further research confirming SMEs are often the target of cyber-attacks on data[40], adherence will in many cases represent a significant challenge. There will be required changes in organisational attitudes towards effective data integrity and cyber security, and support to companies that lack the appropriate resources of skillsets to implement effective security practices.

To some extent, Brazil does have a second-mover advantage, with the ability to observe and analyse how GDPR was implemented and is managed by national DPAs. By aligning major principles of the legislation to existing international legislation such as GDPR Brazil may be able to adopt and adapt existing implementation guidance relating to data transfers. In July 2019 the Information Commissioner's Office (ICO), the UK's DPA, released a Draft Code for Consultation on 'Data Sharing: A Code of Practice'[41], updated to reflect the implications of the UK Data Protection Bill (which enshrined GDPR into UK law) and offering practical guidance for organisations on how to share personal data in adherence with the Bill. It is highly advised that the ANPD draft and release similar guidance, with the recognition that without sufficient adherence to the legislation, any complications in data transfers will affect international business opportunities, an effect only exaggerated by the opportunities offered by the EU-MERCOSUR trade agreement. Similarly, a lack of adherence over time may challenge any long-lasting adequacy decision achieved by Brazil by the European Commission; adequacy decisions may be revoked at any time and there is therefore a requirement to consistently demonstrate adequacy regarding data protection.

---

[38] ENISA *Guidelines for SMEs on the security of personal data processing:* https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing <Accessed 30 July 2019>

[39] Data Protection: Better Rules for Small Businesses *EU Commission:* https://ec.europa.eu/justice/smedataprotect/index_en.htm <Accessed 30 July 2019>

[40] AssessProPr *LGPD and SMEs: short-term impacts:* https://www.assespropr.org.br/en/lgpd-e-as-pmes-impactos-de-curto-prazo/ <Accessed 1 August 2019>

[41] Data Sharing: A Code of Practice - UK Information Commissioner's Office: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf <Accessed 30 July 2019>

Conclusion

There are many opportunities available to Brazil with the implementation of MERCOSUR - which could be amplified by effective and efficient data transfer mechanisms. It is in Brazil's interest to create strong data protection legislation that can demonstrate secure handling of international data transfers and reassure trade partners. Furthermore, Brazil has correctly drawn inspiration from the regulations of both Latin American colleagues and the European Union, reducing the challenges of adhering to multiple regulatory frameworks and encouraging further integration in trading and data exchange.

While the final formation of Brazil's data protection authority is yet to be announced, one of the goals of the authority (and of involved stakeholders across Brazil) will be to meet the EC's adequacy requirements and integrate themselves into the growing network of states with comprehensive data protection legislation.

The establishment of a network of States with adequate level of protection is crucial for securing the free flow of data and facilitating international trade. This is surely important for Brazil *vis-à-vis* European countries, but also a Member of MERCOSUR. Mutual acknowledgements of adequacy can facilitate immensely the data transfer and by extension, trade.