Personal Data Protection and Data Transfer Regulation in Brazil

By Pablo Trigo Kramcsák
Contents

Summary ................................................................................................................................................. 3
1 Context .................................................................................................................................................. 4
2 Brazil’s Data Protection Model ............................................................................................................. 5
   2.1 Personal Data Protection as a Fundamental Right ........................................................................ 5
   2.2 Relevant General Rules .................................................................................................................. 6
   2.3 Comprehensive Data Protection Law. The LGPD ........................................................................ 7
   2.4 Influence of the GDPR Model on the LGPD ............................................................................... 8
   2.5 Core of the LGPD ........................................................................................................................... 9
      2.5.1 Personal Data under the LGPD ............................................................................................. 9
      2.5.2 Scope ..................................................................................................................................... 10
      2.5.3 Data Processing Principles .................................................................................................... 12
      2.5.4 Data Subject’s Rights ............................................................................................................. 12
      2.5.5 Lawful Grounds for Data Processing ....................................................................................... 13
      2.5.6 Data Protection Authority ....................................................................................................... 14
      2.5.7 Other Elements ....................................................................................................................... 15
   2.6 Data Retention and Data Localisation ........................................................................................... 15
      2.6.1 Internet Bill of Rights .......................................................................................................... 15
      2.6.2 Cybersecurity and Cloud Rules ............................................................................................. 16
   2.7 Surveillance and Law Enforcement Rules ...................................................................................... 17
3 Transfer of Personal Data to Third Countries .................................................................................... 19
   3.1 Scope ............................................................................................................................................. 19
   3.2 Data Transfer Tools ......................................................................................................................... 19
   3.3 Recent Evolution ............................................................................................................................. 20
4 International Commitments ................................................................................................................ 22
5 Conclusions ........................................................................................................................................... 28

The Brussels Privacy Hub publications are intended to circulate research in progress for comment and discussion. Available at https://brusselsprivacyhub.com/. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged.

DISCLAIMER
The opinions expressed in this paper are those of the author/s.
Summary
Brazil is a major global actor, leading South-South cooperation and forging strategic partnerships with China and the European Union. The country holds a prominent position in the digital sphere, standing as Latin America's largest e-commerce market and an important hub for data centers.

In response to the need for comprehensive data protection regulations, Brazil enacted the Brazilian General Data Protection Law (LGPD) in September 2020. The EU General Data Protection Regulation (GDPR) served as a model for the LGPD, and both laws have many common features.

The LGPD is the cornerstone of Brazil's data protection framework, presenting a wide-ranging material scope and establishing a comprehensive set of data processing principles, rights and obligations. Following the GDPR's approach, the LGPD has a broad extraterritorial reach. The Brazilian Data Protection Authority, the ANPD, plays a crucial role ensuring compliance with LGPD provisions.

Chapter V of the LGPD addresses international data transfers, establishing a range of guarantees and safeguards designed to protect the rights of individuals whose data is being exported. To begin with, the LGPD permits these transfers if the destination country maintains an adequate level of protection, as assessed by the ANPD.

Beyond countries with an adequate protection level, the LGPD allows cross-border data transfers under specific circumstances, when the controller offers and proves guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided in the LGPD. These situations include: controller’s specific contractual clauses for a given transfer; standard contractual clauses (SCCs), prepared and approved by the ANPD establish minimum guarantees and valid conditions for carrying out an international data transfer; binding corporate rules; or seals, certificates and codes of conduct. The LGPD does not specify a hierarchical order among the available options for cross-border data transfers.

The ANPD released on August 15, 2023, a draft regulation on data transfers. This draft establishes special requirements and guarantees for data exports, defines the content of SCCs, outlines the analysis process for specific contractual clauses and binding corporate rules, and specifies the adequacy decision assessment process for the data protection equivalence of foreign countries or international organizations. This draft also outlines procedures for the ANPD's recognition of equivalence for SCCs from other countries or international organizations, with an emphasis on prioritizing approval for widely applicable clauses. Additionally, it proposes a template for SCCs.

It can be argued that SSCs will play a crucial role in Brazilian LGPD international data transfer framework, standardizing data protection obligations between data exporters and importers, ensuring compliance with LGPD principles even when transferring data to countries lacking an adequacy status. The ANPD's draft regulation on data transfers outlines a simplified procedure for ANPD's recognition of equivalence for standard contractual clauses from other countries or international organizations (a process that may be initiated ex officio or upon the request of the interested parties), emphasizing approval prioritization for widely applicable SCCs.
1 Context

Brazil is one of the largest economies in the world, with a significant impact on international trade, investment, and economic cooperation. Its rich natural resources, varied industries, and emerging markets make Brazil a key player in shaping global economic trends and building collaborations.

As a leading nation in Latin America, Brazil has promoted economic and diplomatic integration in the hemisphere. It has also advocated for the interests of developing countries (the Global South) on the world stage. Moreover, Brazil is a key driver of the Southern Common Market (MERCOSUR) trade bloc, which aims to achieve economic integration with Argentina, Paraguay, and Uruguay.¹

Beyond the Latin American sphere, Brazil holds significant political and economic sway as an emerging global power. It collaborates closely with China, India, and Russia, often through alliances such as the BRICS informal group. It is also a member of the G20, an intergovernmental forum that brings together the world’s 20 largest economies. Brazil’s strategic position in the World Trade Organization (WTO) aims to reduce Western dominance and strengthen alternative global structures.²

Brazil maintains robust economic ties with major players such as China, the United States (US), and the European Union (EU). China serves as its principal trade partner. In 2022, their bilateral trade reached approximately USD 150 billion, absorbing nearly 27% of Brazil’s export volume.³ Brazil aims to enhance and broaden its trade connections with China.⁴ The EU is Brazil’s second-biggest trading partner, accounting for 18.3% of its total trade, and the biggest foreign investor in Brazil.⁵

Brazil’s South-South diplomacy has placed significant importance on the African continent, particularly emphasizing relationships with Portuguese-speaking African countries, Nigeria, and South Africa.⁶ In this sense, Brazil has expanded its partnerships with various regional or sub-regional African organisations through bilateral agreements, reflecting its pursuit of a more proactive role on the continent.⁷

---

⁴ McIlhenny (n 2).
Brazil is a significant player in the digital sphere, establishing itself as the largest e-commerce market in Latin America.\textsuperscript{8} It is also the seventh most populous country in the world,\textsuperscript{9} with a large digital community of about 181.8 million internet users,\textsuperscript{10} ranking fifth globally.\textsuperscript{11}

The country stands out as the primary data centre market in Latin America, attracting approximately 50% of the region’s total investment. Sao Paulo is a key hub for data centre facilities, hyperscale infrastructure, and cloud regions in the country. Leading cloud service providers such as AWS, Microsoft, Oracle, IBM, Tencent, and Huawei have a strategic presence in Brazil, offering private and public cloud services, mainly for the financial and government sectors.\textsuperscript{12}

Brazil has been developing its regulatory frameworks to adapt to the digital era. In recent years, Brazil has enacted data protection laws to protect the privacy and rights of its digital citizens. The Brazilian General Data Protection Law, which follows the EU’s General Data Protection Regulation (GDPR), shows the country’s commitment ‘to increase the protection of personal data and regulate the way businesses collect, use, and process personal data’.\textsuperscript{13} This legal framework regulates the processing of personal data, bringing Brazil in line with the highest international data protection standards.

2 Brazil’s Data Protection Model

2.1 Personal Data Protection as a Fundamental Right

It is relevant to highlight the connection between international human rights law, particularly the right to personal data protection, and Brazil’s legal and constitutional framework.\textsuperscript{14}

The 1988 Constitution of the Federative Republic of Brazil (Federal Constitution) establishes privacy as fundamental constitutional right. Article 5(X) of the Federal Constitution safeguards the inviolability of individuals’ privacy, private life, honour, and image. It also ensures the right to compensation for both material and moral damages caused by any violation of these rights.


Additionally, on 10 February 2022, the Federal Senate approved Constitutional Amendment No. 115/2022, which specifically added personal data protection, including in digital means, into the list of fundamental rights outlined in Article 5 of the Federal Constitution. The amendment emphasises that the Federal Government has exclusive authority to oversee personal data protection issues, ensuring that only federal laws regulate the protection and processing of personal data. This centralised approach seeks to prevent inconsistency caused by different laws at the state and city levels.\(^\text{15}\)

Furthermore, the Constitution contains the habeas data provision (Article 5(LXXII)(a)), which guarantees the rights of individuals to have access to their personal information contained in registries or databases maintained by the Federal Government or other public entities and to demand the correction of any incorrect data. The habeas data writ (regulated by the Habeas Data Law No. 9,507/1997) is a constitutional remedy and ‘not strictly a substantive right, although this aspect can be inferred through its characteristics’.\(^\text{16}\) It is worth noting that the habeas data writ ‘has influenced other Latin American countries who have implemented similar data protection instruments’.\(^\text{17}\)

2.2 Relevant General Rules

The general data protection and privacy framework in Brazil encompasses several legislative sources, including the Brazilian Civil Code, the Consumer Protection Code, and the Internet Bill of Rights,\(^\text{18}\) having ‘more than 40 laws and norms at the federal level’.\(^\text{19}\)

It’s worth noting that ‘Brazil does have a strong civil law tradition and a developing consumer protection culture’, with the Civil Code giving ‘the contour the right to privacy, private life, home, correspondence and


\(^{16}\) Borges (n 14).


reputation’. The Brazilian Civil Code, Law No. 10,406/2002, establishes privacy as an inviolable right of individuals (as stipulated in Article 21 of the Civil Code) and allows for civil action. The Consumer Protection Code (Law No. 8,078/1990) also regulates the processing of consumer data. It gives consumers the right to access their own data, as specified in Article 43. This legislation is applicable to the collection and administration of databases containing consumers’ personal information, including Internet users. Additionally, the Internet Bill of Rights (Law No. 12,965/2014) establishes principles, rights and obligations that service providers, including infrastructure and platforms, must follow. It contains specific rules related to the processing of personal data in online contexts.

2.3 Comprehensive Data Protection Law. The LGPD

The Brazilian General Data Protection Law No. 13,709/2018 (Lei Geral de Proteção de Dados or LGPD) came into effect on August 16, 2020, retroactively from its enactment on September 18, 2020. The process of creating a comprehensive data protection law began in 2010, when the national consumer secretary of the Ministry of Justice presented a draft bill on data protection for public consultation. Brazil lacked a comprehensive framework for protecting personal data before the LGPD came into effect. Its data protection strategy was mainly based on different regulations for each sector, as explained in the previous sections. This situation might have limited Brazil’s potential to excel in the digital economy, as it lacked a strong data protection framework that could foster its development. The implementation of the LGPD stands as a critical measure to confront this issue, in order to fill the gaps in privacy and data protection regulations, creating a legal environment conducive to Brazil maximising its potential in the data-driven economy.

The LGPD applies horizontally, and its far-reaching provisions cover the activities of data controllers and processors, establishing novel requirements for the processing of information of data subjects. The LGPD addresses various critical aspects, encompassing robust principles, guidelines for extraterritorial application, strong security measures, management of cross-border data transfers, mandates for appointing data

---

22 Privacy International and Coding Rights (n 17).
24 We will refer in detail to these provisions in section 2.6(a).
protection officers and conducting data protection impact assessments. ‘These provisions uniform and complement the existing data protection framework’.  

It is enforced by the National Data Protection Authority (Autoridade Nacional de Proteção de Dados or ANPD), which provides important guidance and clarity on the provisions of the LGPD. The LGPD entrusts the ANPD with significant interpretation, application, and enforcement responsibilities. Consequently, the effectiveness and success of this law relies heavily on the central role played by the ANPD.

2.4 Influence of the GDPR Model on the LGPD

Brazil and the EU share strong historical, cultural, and economic bonds. Brazil was the first Latin American nation to forge diplomatic ties with the European Economic Community. Politically, Brazil and the EU acknowledge their roles as participants in a multipolar and evolving global system. In this sense, improving relationships between the EU and Latin America holds strategic importance for Europe, and closer ties between the EU and Brazil might hold significant potential.

There has been a trend of replicating or transplanting European regulatory frameworks into the Global South for various reasons, including what is known as the "Brussels Effect". Brazil has also endeavoured to 'align itself with international standards and references through these approaches'. In that connection, ‘the LGPD is largely inspired by the European data protection model’. The GDPR significantly influenced the Brazilian data protection law by exporting European data protection standards.

This impact is notably apparent in the broad integration of GDPR principles into Brazil’s LGPD. The LGPD was formulated with the GDPR as a foundational reference to such an extent that it is often regarded as Brazil’s GDPR. The LGPD aims to safeguard individual rights while fostering economic, technological, and

---

28 Privacy International and Coding Rights (n 17).
33 Borges (n 14).
35 Canaan (n 32).
36 Borges (n 14).
37 Renato Opice Blum and Camilla Rioja, ‘Brazil’s “GDPR” Sanctioned with Extraterritorial Effects’ (2018) IEEE Internet Policy Newsletter, September 2018
innovative advancements by implementing clear, transparent, and comprehensive regulations for the appropriate handling of personal data. These objectives closely mirror the goals outlined in the GDPR.\(^{38}\)

The LGPD comprises 65 articles that grant individuals specific rights regarding their data, place responsibilities on organisations for the lawful processing of personal information, mandate the reporting of data breaches to both the supervisory authority and affected individuals, oversee the international transfer of data, and enforce penalties akin to those outlined in the GDPR. In this sense, the Brazilian data protection law replicates key points of the European regulation. For instance, the LGPD presents a broad international scope, with Article 3 LGPD adopting the marketplace location principle, 'whereby the offering of goods or services or processing of data aimed at individuals located on Brazilian territory is enough for applicability'.\(^{39}\)

However, it also contains some particularities adapted to Brazil. While ‘the legal frameworks about data protection share foundational aspects across Brazil and Europe, cultural, historical, and legal contexts give rise to nuanced divergences in their implementation’.\(^{40}\) For example, the Brazilian law creates ten legal bases allowing the processing of personal data, including credit protection. The credit protection lawful ground is specifically adapted to Brazil's credit sector's needs. Considering that the LGPD includes additional legal grounds for data processing, it could be possible to consider Brazil’s data protection law ‘as more flexible and less restrictive than GDPR in relation to the processing of personal data’.\(^{41}\)

2.5 Core of the LGPD

2.5.1 Personal Data under the LGPD

The LGPD has established a unified data protection framework, imposing general obligations across all sectors while ‘systematizing the rights of data subjects’.\(^{42}\)

Within the LGPD, the concept of personal data is broadly defined, encompassing any information about an identifiable individual (Article 5(I)). This definition is not solely confined to information directly identifying an individual but also data that could potentially identify the person when aggregated with other information. Moreover, given their susceptibility to discriminatory practices, the LGPD introduces specific provisions targeted at sensitive personal data. This category includes personal data concerning racial or ethnic origin, religious beliefs, political opinions, trade union or religious, philosophical, or political organisation membership, health or sex life, and genetic or biometric data when linked to a natural person.

According to Article 12 of the LGPD, anonymized data is not deemed as personal data, except in cases where the anonymization process can be reversed through appropriate means or with reasonable efforts. The assessment of what constitutes ‘reasonable’ must consider objective factors including costs, time, available technology, and the sole use of internal means required to reverse anonymization. The ANPD may provide

\(^{38}\) Abigayle Erickson, ‘Comparative Analysis of the EU’s GDPR and Brazil’s LGPD: Enforcement Challenges with the LGPD’ (2019) 44 Brook. J. Int’l L. 859.

\(^{39}\) Hoffmann and Vargas (n 21).

\(^{40}\) Borges (n 14).


for standards and techniques to be used in processes of anonymization and carry out security checks. It should be noted that according to Article 12, paragraph 2, ‘the data used for formation of the behavioral profile of a given natural person, if identified, may also be deemed personal data’. Unlike the GDPR, the LGPD has not sufficiently systematized the concept of pseudonymization, nor has it formulated explicit incentives for its adoption by data processing agents.

On January 30, 2024, the ANPD published, for public consultation, a Preliminary Study on anonymization and pseudonymization for data protection. The study will inform the future guidelines on these topics, which aim to guide the processing agents on the legal impacts and the various techniques to anonymize or pseudonymize personal data. The study emphasizes that anonymization and pseudonymization are not one-time actions, but continuous processes based on a risk approach. Therefore, they need to be constantly reevaluated to ensure that the risk of reidentification of the data subjects is acceptable, considering the speed of technological advancement, the availability of auxiliary data and the sophistication of possible attacks. The study mentions that any anonymization process must be accompanied by a documented risk management, based on techniques to measure the risk of reidentification of data, such as k-anonymity. These techniques must take into account the cost and time required to reidentify the data, as well as the context of the existing technologies, the nature, scope, context and purpose of each processing operation. Finally, the study provides in Annex II examples of anonymization and pseudonymization techniques, based on the type of data, distinguishing between structured text and images.

In addition, it’s worth noting ANPD Technical Note No. 46/2022/CGF/ANPD from May 2022. In this note, the ANPD makes some considerations regarding the anonymization process, and recalls that anonymization is neither a panacea nor the only form of data protection. In this vein, it notes that anonymization does not reduce the probability of re-identification of a data set to zero. Although full anonymization is a desirable objective from a personal data protection perspective, in some cases this is not possible and must be considered a residual risk of re-identification (point 5.21). Moreover, the ANPD explicitly mentions two anonymization techniques: k-anonymity (point 5.24) and differential privacy (point 5.25).

2.5.2 Scope
The LGPD applies broadly to any processing operation carried out by a natural person or a legal entity of either public or private law, irrespective of the means, the country in which its headquarters is located or the country where the data are located. The term “processing” is extensively defined in Article 5(X) and covers a wide range of activities involving personal data. These activities include collecting, producing, receiving, classifying, using, accessing, reproducing, transmitting, distributing, storing, deleting, evaluating, controlling, modifying, communicating, transferring, disseminating, or extracting information.

43 Pseudonymization is defined in Article 13, paragraph 3, LGPD as the processing by means of which data can no longer be directly or indirectly associated with an individual, except by using additional information kept separately by the controller in a controlled and secure environment.
45 Available at https://www.gov.br/participamaisbrasil/consulta-a-sociedade-estudo-preliminar-anonimizacao-e-pseudonimizacao-para-protecao-de-dados
Following the GDPR’s approach, the LGPD exhibits a broad extraterritorial scope. As outlined in Article 3, the law applies to any processing activity, regardless of where the organisation collecting the data is established, if: (i) the processing is carried out in Brazil; (ii) the processing aims to provide goods or services or to process data of people in Brazil; or (iii) the data has been collected in Brazil. Consequently, the country in which the company is based becomes inconsequential as long as one of these criteria is met, making the LGPD fully enforceable regardless of the company’s headquarters’ location. Unlike the GDPR, which requires foreign companies to designate a representative in the EU under Article 27 when they are subject to its rules, the LGPD does not impose such an obligation on processing agents not established in Brazil.\(^{48}\)

In Article 4, the law excludes the application of data processing regulations in specific scenarios, namely: (i) data processing made by a natural person for exclusively private and non-economic purposes; (ii) data processing made exclusively for journalistic, artistic or academic purposes; (iii) data processing made exclusively for the purposes of public security, national defense, safety of the Country, or crime investigation and punishment activities (subject to specific legislation);\(^{49}\) and (iv) ‘data originating from outside the Brazilian territory and which are not subject to communication, shared use of data with Brazilian processing agents or subject to international transfer of data with other country than the country of origin, provided the country of origin provides a degree of personal data protection consistent with LGPD provisions’.\(^{50}\)

It is important to mention that the LGPD does not completely exclude data processing for academic purposes. Processing agents still need to follow the conditions laid out in Article 7 (covering lawful bases and other requirements for processing personal data) and Article 11 (on the processing of sensitive personal data) of


\(^{49}\) We will refer in detail to this provision in section 2.7.

the Law.\textsuperscript{51} In reference to the circumstance delineated in Article 4(IV), which involves a type of transient data transfer, there is ‘no equivalent provision in the GDPR’,\textsuperscript{52} involving a type of transient data transfer.

\subsection*{2.5.3 Data Processing Principles}

The Brazilian General Data Protection Law embodies 10 fundamental principles (Article 6) that underpin the processing of personal data. These principles serve as the cornerstone of Brasil’s data protection framework, advocating for purpose limitation, adequacy or compatibility of the processing with the purposes communicated to the data subject, necessity or data minimisation, free access to the data subjects, data quality, transparency, data security, prevention of damage, non-discrimination and accountability.

\subsection*{2.5.4 Data Subject’s Rights}

LGPD gives individuals a set of 9 rights (Article 18), empowering them to exert control over their personal data vis-à-vis both public and private entities subject to the LGPD. These rights are the right to be informed about the existence of the processing; the right to access the data, the right to correct inaccurate, incomplete, or out-of-date data; the right to block, anonymise, or delete excessive or unnecessary data or data that is not being processed in compliance with LGPD; the right to the portability of data to another service by an express request; the right to deletion of personal data which is processed with the consent of the data subject; the right to information about private and public entities with which the data is shared; the right to be informed about the possibility of denying consent and the consequences of such denial; and the right to revoke consent.

Data subjects are afforded additional rights elsewhere in the LGPD.\textsuperscript{53} For example, Article 8 ensures accessible and transparent access to comprehensive information concerning the processing of personal data, mandating clear and adequate disclosure. Meanwhile, Article 20 gives data subjects the right to request review of decisions made solely based on the automatized processing of personal data that affects their interests, including of decisions designed to define their personal, consumption and credit profile or aspects

\textsuperscript{51} The LGPD does not define these academic purposes. There are uncertainties surrounding the definition and scope of data processing made exclusively for academic purposes. The ANPD’s Guidance - Processing of personal data for academic purposes and for carrying out studies and research (2023) points out that this concept is closely tied to the exercise of academic freedom by professors, students, and researchers within research bodies or educational institutions, in environments that foster the exchange and discussion of ideas, such as classrooms, scientific congresses, and seminars. Partial derogation for academic purposes should be interpreted restrictively, applying only to situations where the processing of personal data is directly related to the exercise of academic freedom, and it would not apply if personal data processing serves other purposes, even indirectly related to academic activities, such as administrative or commercial functions within educational institutions. (Andressa Girotto Vargas, Augusto Henrique Alves Rabelo, Diego Vasconcelos Costa, Fernando de Mattos Maciel, Gustavo Gonçalinho, Lucas Borges de Carvalho and Sabrina Fernandes Maciel Favero, ‘Guia orientativo - Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas’ (2023) ANPD Autoridade Nacional de Proteção de Dados (June 2023) Available at https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf). At the same time, it can be estimated that the extent of this exclusion is not clear. For instance, the ANPD’s Guidance - Processing of personal data for academic purposes and for carrying out studies and research, asserts (on page 22) that the fact that the processing of personal data for academic purposes to be supported by one of the legal grounds contained in Article 7 LGPD does not mean that other LGPD provisions are not applicable, mentioning, by way of example, provisions relating to the data subjects’ rights.

\textsuperscript{52} OneTrust DataGuidance and Baptista Luz Advogados (n 13).

\textsuperscript{53} Belli, Lorenzon and Fergus (n 50)
of their personality. It is framed as a ‘right to review’, ‘thereby allowing for indirect control’ of automated decision making.\(^{54}\)

### 2.5.5 Lawful Grounds for Data Processing

The LGPD establishes 10 legal bases for lawful data processing (Article 7): (i) data subject’s consent; (ii) for compliance with a statutory or regulatory obligation by the controller; (iii) by the public administration, for the processing and shared use of data required for the performance of public policies set forth in laws or regulations or supported by contracts, agreements or similar instruments; (iv) for conducting studies by research bodies;\(^{55}\) guaranteeing, whenever possible, the anonymization of personal data; (v) when necessary for the performance of agreements or preliminary procedures relating to agreements to which the data subject is a party, at the request of the data subject; (vi) for the regular exercise of rights in lawsuits, administrative or arbitration proceedings; (vii) for protection of the life or of the physical safety of the data subject or of third parties; (viii) for health protection, exclusively, in a procedure performed by health professionals, health services or health authorities; (ix) when necessary to serve the legitimate interests of

\(^{54}\) Hoffmann and Vargas (n 21). ‘The wording of this provision seems to suggest a wider protection than the relevant Article 22 of the GDPR which requires that the decision “has a legal effect or significantly affects the data subject”’ (Katerina Demetzou, ‘At the Intersection of AI and Data Protection Law: Automated Decision-Making Rules, a Global Perspective (CPDP LatAm Panel)’ (www.fpf.org, 30 July 2021) <https://fpf.org/blog/at-the-intersection-of-ai-and-data-protection-law-automated-decision-making-rules-a-global-perspective-cpdp-latam-panel/> accessed 20 December 2023.). However, the provision of Article 20 of the LGPD would not operate as a general prohibition of individual decisions based 'solely' on automated processing.

\(^{55}\) Although the LGPD establishes a more flexible legal regime for the processing of personal data for research purposes, it does not explicitly define the concepts of "study" or "research". It should be noted, however, that Article 5 offers a narrow definition for a ‘research body.’ This is relevant, given that the ‘legal basis of ‘research’ is only valid for studies conducted by research bodies that meet the definition’ (OneTrust DataGuidance and Baptista Luz Advogados (n 13)). According to Article 5(XVIII) LGPD, a research body is a ‘body or entity of the direct or indirect public administration or not-for-profit legal entity governed by private law organized under the Brazilian laws, with its headquarters in Brazil, that includes basic or applied research of a historical, scientific, technological or statistical character in its institutional mission or bylaw’. When research bodies engage in data processing for purposes other than conducting studies, they must rely on a different legal basis (Andressa Girotto Vargas, Augusto Henrique Alves Rabelo, Diego Vasconcelos Costa, Fernando de Mattos Maciel, Gustavo Gonçalinho, Lucas Borges de Carvalho and Sabrina Fernandes Maciel Favero, ‘Guia orientativo - Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas’ (2023) ANPD Autoridade Nacional de Proteção de Dados (June 2023) Available at https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf).

Regarding sensitive data, Article 11 LGPD establishes that this category of data can only be processed in certain circumstances without the supply of the data subjects’ consent, including when this is essential for the conduction of studies by research bodies, ‘guaranteeing, whenever possible, anonymization of the sensitive personal data (Article 11(ii)(c)). In addition, article 13 LGPD states that in the ‘conduction of studies on public health, the research bodies may have access to personal databases, which shall be exclusively processed within those bodies and for the sole purpose of conduction of studies and researches, and they must always be kept in a controlled and safe environment, according to the security practices set forth in the specific regulations and which include, whenever possible, the anonymization or pseudonymization of the data, and which consider the due ethical standards relating to studies and researches.’
the controller or of third parties, except in the event of prevalence of fundamental rights and liberties of the data subject; and (x) for the protection of credit.56

These requirements come hand in hand with strict obligations for organizations to uphold mandatory and transparent disclosures within their privacy policies. Further, the law delineates special provisions for the processing of sensitive personal data (Article 11) and children’s data protection (Article 14). Due to the sensitivity of this information, the LGPD outlines limited circumstances under which such data may be processed.57

2.5.6 Data Protection Authority
The National Data Protection Authority of Brazil operates as a federal public administration body. Provisory Measure No. 1124/2022,58 later transformed into Law No. 14,460/2022,59 brought changes to the LGPD and transformed the ANPD into a ‘special nature autarchy’.60 This change granted the ANPD autonomy and independence in making decisions and issuing normative publications. Subsequently, the Presidential Decree No. 11,348/2023, connected the ANPD to the Brazilian Ministry of Justice and Public Safety. This action ended its previous direct affiliation with the Presidency of the Republic.61 Constituted at the end of 2020, it is considered an independent data protection authority,62 with a ‘solid regulatory and personnel structure’.63

ANPD objectives encompass various aspects, including:

- Interpreting and clarifying the LGPD.
- Developing regulations for LGPD application and staying updated with evolving technologies and trends.
- Collaborating with other regulatory bodies and overseeing public authorities subject to the LGPD.
- Evaluating other jurisdictions to assess if they adequately protect data subjects’ data.
- Regulating cross-border data transfers.
- Handling data subjects’ complaints and enforcing the LGPD.
- Conducting investigations, holding hearings, and enforcing sanctions and penalties against organizations found to violate the LGPD.

56 Belli, Lorenzon and Fergus (n 50)
57 Rippy (n 19).
58 Available at https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=515&pagina=2&data=14/06/2022
63 Drechsler et al. (n 61).
2.5.7 Other Elements

LGPD’s Articles 37 to 40 define duties in processing personal data: record-keeping. Data Protection Impact Assessments (DPIAs) at the request of the ANPD, obligations to notify specific events such as data breaches, and proper processing practices. To comply, all controllers (public or private entities processing personal data) must appoint a Data Protection Officer (DPO).

When there’s a breach of the LGPD by a controller or data processor, they face redress mechanisms and administrative sanctions imposed by the ANPD. The potential administrative sanctions include imposing fines of up to 2% of the entity’s income in Brazil in the last fiscal year, capped at R$ 50,000,000 for the violation, suspending the processing of data associated with the violation until rectification, and mandating the deletion of personal data linked to the violation (Article 52 LGPD). According to Article 22, the defence of data subjects’ interests and rights may be exercised in court, individually or collectively.

Article 42 of the LGPD establishes civil liability for the controller or processor engaging in data processing activities that result in property, moral, individual, or collective harm due to violations of the law.

2.6 Data Retention and Data Localisation

There is no provision for data localization in Brazilian federal law. There are sectoral regulations that include ‘data localization as a requirement for public procurement contracts involving cloud-computing services’. These provisions are found in norms of the Secretary of Information Technology of the Ministry of Planning, Development, and Management ‘regarding government contracts related to information and communications, which may include encryption methods, firewalls, and other measures. According to these rules, confidential data or information produced or safeguarded by the Federal Public Administration, including backup data, shall be physically located in Brazil’.

2.6.1 Internet Bill of Rights

Brazil’s Internet Bill of Rights, Law No. 12,965/2014, provides for broad internet users’ rights like the protection of their privacy and private communications, the protection of personal data, the right to obtain information on the collection, storage and processing of their data, the right to erase data, among others. The Internet Bill of Rights emphasizes key privacy protection principles, notably affirming privacy rights (Article 3). It acknowledges the confidentiality of online communications, permitting exceptions solely through court orders in criminal investigations or procedures (Article 7(I)). Moreover, it guarantees the right

---

64 While the GDPR precisely outlines in Article 30 the information to be recorded, the LGPD lacks specific details in this regard (OneTrust DataGuidance and Baptista Luz Advogados (n 13)).

65 According to Article 5(XVII) LGPD, the DPIA is a document elaborated by the controller that contains a description of the personal data processing processes that could generate risks to civil liberties and to fundamental rights, as well as measures, safeguards and mechanisms to mitigate these risks. Even though they are not initially mandatory, DPIAs must be provided to the ANPD upon request (Article 38 LGPD).


to accessible and transparent privacy policies (Article 7(IV)). Article 11 establishes that ‘[a]ll operations involving the collection, storage, retention or processing of records, personal data, or communications by Internet service and applications providers must comply with Brazilian law and the rights to privacy, protection of personal data, and confidentiality of private communications and records, if any of those acts occur in Brazilian territory’. The law includes a requirement that internet services providers and other internet services retain user data for a year and six months respectively. In this sense, the Internet Bill of Rights is ‘a standard for the improvement of current practices of data retention in Brazil’.72

In 2016, the Regulatory Decree No. 8,771/2016 was enacted to clarify some provisions of the Internet Bill of Rights.73 This decree primarily focuses on preserving net neutrality while also tackling certain aspects of privacy and confidentiality. Specifically, it mandates the minimal retention of personal data and private correspondence.74 The Regulatory Decree also provides for the obligation to safeguard personal data by means of adequate information security measures, including the adoption of strict control of the employees who access personal data (access control). In addition, it establishes rules on purpose limitation and adequate use of personal data when processed via the Internet, noting that data must be eliminated when it achieves the purposes of its processing.

2.6.2 Cybersecurity and Cloud Rules

On December 29th, 2023, Brazil published its National Cybersecurity Policy (Decree No. 11,856/2023) to guide cybersecurity activities in the country.75 This policy defines a set of principles, including national sovereignty and the prioritization of national interests. It also emphasizes the guarantee of fundamental rights, particularly freedom of expression, protection of personal data, privacy, and access to information.

The decree establishes the National Cybersecurity Committee, which comprises representatives from government, civil society, academic institutions, and business sector organizations. This committee will play a key role in proposing updates to the National Cybersecurity Policy and developing a National Cyber Security Strategy as well as a National Cyber Security Plan.

Furthermore, in the financial sector, banking and finance institutions must also rely on cybersecurity and cloud requirements typically provided by regulatory agencies such as the Central Bank of Brazil (CBB). CBB Resolution No. 4,893/2021 and Resolution No. 85/2021 regulate how financial and payment institutions adopt cybersecurity measures, and the requirements for contracting cloud computing services.

---


74 Erickson (n 38).

75 Available at https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm


77 Available at https://www.bcb.gov.br/content/about/legislation_norms_docs/CMN_Resolucao_No_4,893_2021.pdf

78 Available at https://www.bcb.gov.br/content/about/legislation_norms_docs/BCB_Resolucao_No_85_2021.pdf
including data processing and data storage services. In this sense, financial institutions can only contract with cloud services providers that are established in countries that have an agreement with the Central Bank of Brazil (CBB). In addition, the countries where financial data is processed must be notified to the CBB.

2.7 Surveillance and Law Enforcement Rules

Article 4(III) of LGPD states that the law ‘shall not apply to the processing of personal data: [...] made exclusively for the following purposes: a) public security; b) national defense; c) safety of the country; or d) crime investigation and punishment activities’. Then, Article 4, paragraph 1, establishes that this kind of data processing ‘shall be governed by a specific law, which shall contain proportional measures as strictly required to serve the public interest, subject to the due process of law, the general principles of protection and the rights of the data subjects set forth in this Law’.

Paragraph 2 of the same article adds that private entities are barred from processing data mentioned in Article 4(III), ‘except in procedures carried out by a legal entity governed by public law’. This process must be specifically notified to the ANPD and must adhere to the limitations set in paragraph 4. Paragraph 4 states that in no event can all personal data of the database set forth in Article 4(III) ‘be processed by a person governed by private law’, unless its capital is entirely owned by public entities. The ANPD holds the responsibility to provide technical opinions or recommendations regarding these exceptions. Moreover, it has the authority to request the entities in charge to conduct data protection impact assessments.

In light of this, ‘[a] future data protection law for public security and criminal prosecution will have to provide for proportionate and strictly necessary measures for fulfilling the public interest, subject to due legal process, and observe the general principles of protection and the rights of the data subject’.81

Considering the rule contained in Article 4, paragraph 1º, LGPD, it is possible to argue that ‘the principles of data protection must already be observed for these activities. The recent recognition of the fundamental right to the protection of personal data by the Brazilian constitution also reinforces the need for minimal safeguards for any processing of personal data in the country’.82

It should be noted that while public intelligence, investigative, and criminal prosecution activities aren’t covered by the LGPD, Chapter V allows these activities as a legal basis for data transfers.83

Brazil has not yet approved specific regulation on personal data processing in law enforcement. ‘Even though there were legislative initiatives to establish a law for regulating the topic, these are still in a very initial stage’.84 One of these initiatives is the Personal Data Protection Bill for the exclusive purposes of state

---

80 ibid.
81 ‘In Brazil, the competence to deal with public security is shared between different levels of the federation and encompasses different bodies, which makes a unique analysis of the use of personal data by these institutions a complex task’ (Drechsler et al. (n 61)).
82 ibid.
83 Drechsler et al. (n 61).
security, national defense, public security, and investigation and repression of criminal offenses (Bill No. 1,515/2022), based on a preliminary draft prepared by a commission of jurists.

A relevant decision by the Brazilian Supreme Federal Court in September 2022 has implications for the legality of data sharing among public authorities. The decision concerned the consolidated cases ADI 6,649 and ADPF 695, which challenged the presidential Decree No. 10,046/2019. The Decree aimed to enable the exchange and integration of data, including non-sensitive and sensitive personal data, among various public entities within the Federal Public Administration. To do so, the Decree created different levels of data sharing. Specific organs would have access to certain databases, as determined by public agents, based only on their confidentiality. The Decree did not define any specific purposes for data sharing. The Court ruled that the federal government must revise the rules on data sharing and interoperability, in accordance with the constitutional right to data protection and privacy. The Court also set out a number of criteria that must be followed by the public administration when sharing data, such as limiting the data to the minimum necessary for the informed purpose, and complying with the requirements, guarantees and procedures established in the LGPD, as far as compatible with the public sector.

Available at https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300

The Bill No. 1,515/2022 addresses data sharing in various scenarios, such as: between competent authorities, between a competent authority and a non-competent public entity, and between competent authorities and private legal entities. The draft does not limit the sharing of personal data between competent authorities and private entities for state security and national defense purposes. For public security purposes, the draft allows competent authorities to access personal data and databases controlled by private legal persons (art. 12) by any of the following means: legal provision; voluntary cooperation; or contract, cooperation agreement or similar instruments. For criminal investigation and prosecution purposes, the draft authorizes a broad range of data sharing (art. 18). Unlike public security purposes, the draft requires a request from the police chief or the Public Prosecutor’s Office instead of a legal provision. The draft also allows data sharing through voluntary cooperation; contract, cooperation agreement or similar instruments; or a state intelligence technical channel (Cynthia Picolo Gonzaga de Azevedo, Eliz Marina Bariviera de Lima, Felipe Rocha da Silva, Gustavo Ramos Rodrigues, Luiza Corrêa de Magalhães Dutra, Paulo Rená da Silva Santarém and Victor Barbieri Vieira Rodrigues, ‘Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022’ (2022) Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), 17. Available at https://lapin.org.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-15152022-1.pdf).

It worth noting that the draft bill has been criticized for changing the initial proposal from the jurists' commission. This has led to concerns about how it affects people’s fundamental rights, disrupts the balance between criminal procedure and data protection principles, and creates legal uncertainty (See Azevedo et al., 2022).

Available at https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=768683585


3 Transfer of Personal Data to Third Countries

3.1 Scope

The transfer of personal data to foreign countries or international entities, as defined in Article 5(XV) LGPD, is regulated by Chapter V of the same law (Articles 33 to 36). The LGPD establishes various guarantees and safeguards to protect the rights of data subjects whose data are processed within the LGPD’s scope (Article 3). If the third country or organization receiving this data does not comply with these safeguards, it may jeopardize the fundamental rights and freedoms of the data subjects.90

These provisions regulate the transfer of personal data by a processing agent (the controller or the processor, as defined in Article 5(IX)), who may be a natural person or a legal entity of public or private law to a data importer (another processing agent, located in a foreign country or which is an international organization, who receives personal data from the exporter).91

3.2 Data Transfer Tools

The LGPD permits international data transfers if the destination country maintains an adequate level of protection, which the ANPD assesses. According to Article 34, this assessment considers: (i) applicable laws in the destination country or international organization; (ii) nature of the transferred data; compliance with personal data protection principles and rights; (iii) security measures aligned with regulations; (iv) legal and institutional safeguards for data protection rights; and (v) any other relevant circumstances for the data transfer.

Furthermore, beyond countries with an adequate protection level, the LGPD allows cross-border data transfers under specific circumstances, when the controller offers and proves guarantees of compliance with the principles and the rights of the data subject and the regime of data protection provided in the LGPD, in the form of: (i) controller’s specific contractual clauses for a given transfer,92 (ii) SCCs (prepared and approved by the ANPD to establish minimum guarantees and valid conditions for carrying out an international data transfer), (iii) global corporate rules,93 or (iv) regularly issued seals, certificates and codes of conduct.

In addition, cross-border transfers are permitted when: (i) it is necessary for international legal cooperation between government intelligence, investigations, and prosecution authorities;94 (ii) it is authorised by the

91 This arises from the provisions contained in the ANPD draft Resolution of the Regulation of International Transfers of Personal Data (released on August 15, 2023 for public consultation).
92 These specific clauses should clearly describe the relationship between the purposes of processing and the international transfer of personal data, indicating the LGPD authorizing hypothesis that substantiates the operation, specifying its purpose, detailing the responsibilities of processing agents and the flow of data, as well as how safeguards for the rights and freedoms of data subjects will be guaranteed. See Zappelini (n 90).
94 It should be noted that while public intelligence, investigative, and criminal prosecution activities aren’t covered by the LGPD, Chapter V allows these activities as a legal basis for data transfers (Drechsler et al. (n 61)).
ANPD; (iii) it is necessary for public policies or public service activities; (iv) data subjects have provided specific and highlighted consent for the transfer upon prior information;\(^95\) (v) it is necessary for the fulfilment of a legal or regulatory obligation on the part of the controller; (vi) it is for a contract or procedures related to a contract in which the data subject is a party, as required by the data subject themself; or (vii) it is for the regular exercise of rights, including contractual performance and in court, administrative, or arbitration proceedings.

According to Article 35, the ANPD is responsible for defining the content of SCCs and verifying the specific contractual clauses for any transfer, as well as the global corporate rules, seals, certificates and codes of conduct. These clauses and rules must comply with the LGPD’s rights, guarantees, and principles. The ANPD can also delegate the assessment of these clauses and rules to certification organizations, as long as they follow its regulation and inspection. The ANPD has the authority to examine and, if needed, modify or cancel the actions of the certification organizations if they don’t align with the law.

Regarding international data transfers, the LGPD and the GDPR have some structural similarities, but they also differ in some respects. For example, unlike the GDPR, the LGPD does not specify a hierarchical order among the available options for international data transfers.\(^96\) Moreover, the LGPD ‘does not provide for the international transfer of data on the basis of a register which is intended to provide information to the public, nor based on the legitimate interest of the controller’.\(^97\)

As Brazil has not yet recognized another country as having an adequate level of data protection and, at the same time, has not yet had this recognition from foreign authorities, each data flow must be evaluated on a case-by-case basis, for consideration of a specific authorization or compensatory measure.\(^98\)

### 3.3 Recent Evolution

On August 15, 2023, the ANPD initiated a public consultation on the regulation of international personal data transfers.\(^99\) This consultation addressed the draft Resolution of the Regulation of International Transfers of Personal Data and the Standard Contractual Clauses (SSCs) template prepared by the ANPD. The draft\(^100\) proposes guidelines for data transfers, emphasising alignment with the Regulatory Agenda for the 2023-2024 biennium (ANPD Ordinance No. 35/2022),\(^101\) which includes actions or initiatives related to international transfers of personal data.

The draft covers important aspects of international data transfers, focusing first on the roles of the data exporter and data importer. The data exporter is a processing agent, located in the national territory or in a foreign country, who transfers personal data to the importer (Article 3.I). Conversely, the data importer is a

---

\(^95\) Regarding the word ”highlighted”, the clause relating to international data transfer cannot be in the middle of other clauses in the case of a contract, and must be separate. See Zappelini (n 90).

\(^96\) Drechsler et al. (n 61).

\(^97\) OneTrust DataGuidance and Baptista Luz Advogados (n 13).

\(^98\) Zappelini (n 90).


\(^100\) Available at https://www.gov.br/participamaisbrasil/regulamento-de-transferencias-internacionais-de-dados-pessoais-e-do-modelo-de-clausulas-padrao-contratuais

\(^101\) Available at https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885
processing agent located in a foreign country or an international organization that receives the personal data transmitted by the exporter (Article 3.II).

The draft defines in Article 3 the concept of “transfer” (processing operation through which a processing agent transmits, shares or provides access to personal data to another processing agent). Then, it distinguishes between international data transfer (the transfer of personal data to a foreign country or to an international organisation of which the country is a member) and international collection of data (the collection of the data subjects’ personal data carried out directly by the processing agent located abroad). According to the draft’s provisions, an international data transfer occurs when personal data moves from an exporter to an importer, distinguishing it from simple international data collection (Article 7 states that international data collection does not characterize international data transfer).

According to Article 2, international data transfer should be carried out: (I) maintaining compliance with principles and data subjects' rights regardless of data location; (II) adopting simple, interoperable procedures that support global standards, economic development, and secure cross-border data flow; (III) implementing responsibility measures to guarantee compliance and accountability; (IV) ensuring transparent information provision to data subjects about transfers; and (V) employing appropriate security measures in line with data criticality and operational risks. Article 9 outlines that international data transfers must be carried out for legitimate, specific, and explicit purposes informed to the data subject, with no possibility of subsequent processing incompatible with such purposes. The transfer must be supported by one of the LGPD’s lawful bases for processing.102

In general terms, the draft Regulation sets the requirements and guarantees for transfers, defines the content of SCCs, outlines the analysis process for specific contractual clauses and global corporate standards (binding corporate rules),103 and establishes an adequacy decision mechanism for foreign countries or international entities' data protection equivalence. It also delineates communication procedures with the ANPD. It should be noted that the draft Regulation does not refer to seals, certificates and codes of conduct.

Article 15 of the draft states that the validity of the international data transfer based on SCCs presupposes the full adoption of the SCCs model prepared by the ANPD (contained in Annex II of the same draft Regulation), without any changes, in a contract between the exporter and the importer. The SCCs can also be part of a specific agreement or a larger agreement to regulate the international data transfer.

Moreover, the draft outlines a simplified procedure for ANPD’s recognition of equivalence for SCCs from other countries or international organizations (a process that may be initiated ex officio or upon the request of the interested parties), emphasizing approval prioritization for widely applicable clauses.104 It is important to note that the ANPD ‘has yet to recognize the equivalence of standard contractual clauses from other countries or international organizations’.105

103 Chapters VI and VII of the draft indicate ANPD’s understanding that global corporate standards are the equivalent to binding corporate rules under the GDPR (see de Oliveira Alves and Scatamacchia (n 102)).
104 It is suggested that this recognition could include SCCs from the EU and the UK. See The Software Alliance (BSA) and the Global Data Alliance (GDA), ‘Response to ANPD Consultation on International Data Transfers’ (globaldataalliance.org, 25 September 2023) <https://globaldataalliance.org/wp-content/uploads/2023/09/09262023intldatatrans.pdf> accessed 13 December 2023.
105 Baker McKenzie (n 99).
The controller is always ultimately responsible for meeting the obligations under the law and the agreement, answering to the ANPD, protecting the data subject’s rights and responding for any damage they may cause, regardless of whether the exporter or importer is in charge of some measures. Also, when both the exporter and importer are processors, the controller must sign the SCCs and take full responsibility for these obligations.\(^{106}\)

It is important to note that in ANPD’s draft SCCs ‘the provisions relating to the rights of the data subject do not provide any limitations, such as those under the EU SCCs’.\(^{107}\) For example, data subjects may file lawsuits against the exporter or the importer, as they choose, before the competent courts in Brazil.

Article 20 of the draft Regulation allows the controller to request the ANPD’s approval for specific contractual clauses for a given transfer, when it involves a unique international data transfer that cannot use the SCCs. This may happen because of exceptional circumstances, factual or legal, that the controller has to justify. The specific contractual clauses must ensure and show compliance with the LGPD principles, the data subjects’ rights, and the data protection framework set by the LGPD and this Regulation.

Regarding global or binding corporate rules, the draft Regulation clarifies that they are intended for international data transfers between organizations of the same economic group, having a binding character upon all members of the group. It states that these corporate standards must be linked to the establishment and implementation of a privacy governance program, enumerating in Article 26 their requisites. These requirements encompass delineating the categories of personal data transferred, specifying the processing objectives, detailing legal frameworks, and identifying the recipient countries. Moreover, the standards must define the corporate structure and responsibilities within the group. They should also explicitly outline the rights of individuals whose data is being transferred and the procedures for exercising these rights, mandating the communication of any alterations to the pertinent data protection authorities.

Finally, on the adequacy decision mechanism, Article 12 specifies that the assessment of the level of protection of personal data ‘shall address the risks and benefits provided by the adequacy decision, acknowledging, inter alia, the guarantee of the principles, the rights of data subjects, and the regime of data protection provided for in the LGPD in addition to the impacts on the international flow of data, diplomatic relations and international cooperation between Brazil and other countries and international organizations’. It also indicates that the ‘ANPD shall prioritize the assessment of the level of data protection of foreign countries or international organizations that ensure reciprocal treatment to Brazil […]’.

The ANPD conducted a public consultation on the draft Regulation for international data transfers until October 14, 2023. The ANPD plans to finalize the regulation process in 2024.\(^{108}\)

### 4 International Commitments

Brazil has ratified several international agreements involving privacy considerations. These include:

---


\(^{107}\) ibid.

• The International Covenant on Civil and Political Rights (ICCPR): Article 17 protects against arbitrary or unlawful intrusion into privacy, family, home, correspondence, and unwarranted attacks on reputation and honour. The Human Rights Committee (the body of independent experts that monitors the implementation of the ICCPR) highlights the obligation of State Parties to the ICCPR to implement legislative measures to uphold these rights.\textsuperscript{109}

• The American Convention on Human Rights, also known as the "Pact of San José de Costa Rica": Article 11 establishes that ‘[n]o one may be the object of arbitrary or abusive interference with his private life’.

• The Council of Europe Convention on Cybercrime (ETS No. 185): On 30 November 2022, Brazil acceded to the Convention on Cybercrime (Budapest Convention).\textsuperscript{110} On 12 April 2023, the Brazilian President signed the corresponding legislative decree, by which Brazil finally adopted the Council of Europe Convention on Cybercrime.\textsuperscript{111}

Furthermore, Brazil has actively contributed to advancing discussions at the United Nations regarding the right to privacy.\textsuperscript{112}

As regards the ‘only binding international convention within the international privacy and data protection policy space’,\textsuperscript{113} Council of Europe’s Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), in 2018, Brazil joined the Committee of Convention 108 as an observer.\textsuperscript{114} With the observer status, Brazil participates in the discussions and workings of the Committee of Convention 108, contributing to the global dialogue and cooperation on data protection and privacy rights.\textsuperscript{115} The main goal of Convention 108 is to enable the free flow of information among Convention Parties

\textsuperscript{109} Coding Rights, Privacy LatAm and Privacy International (n 18).
\textsuperscript{112} Coding Rights, Privacy LatAm and Privacy International (n 18).
\textsuperscript{115} On May 24th, during the 2023 Computers, Privacy and Data Protection International Conference (CPDP), a dedicated panel discussed the anticipated impact of the ratification of the Protocol CETS No 223 amending Convention 108 (also known as the modernised Convention 108 or Convention 108+). Organised by the Council of Europe, the panel included Juliana Muller, Head of International and Institutional Relations at the Brazilian National Data Protection Authority. Muller highlighted the ongoing discussions in Brazil regarding its potential accession to Convention 108. She emphasised that Brazil would now meet the necessary access criteria, specifically highlighting the provisions outlined in article 15.5 of the modernised Convention 108.
and from Parties to non-Parties while safeguarding data protection beyond the jurisdictions of the Parties. The Committee of Convention 108, during its 44th plenary meeting held in Strasbourg from 14 to 16 June 2023, adopted the first module of the Model Contractual Clauses for transborder data flows of personal data developed based on Convention 108+, for data flows from data controller to data controller. At its 45th plenary meeting, the Committee of Convention 108 adopted the second module of the Model Contractual Clauses for transborder data flows of personal data, which addresses the transfer of personal data from controller to processor.

As LGPD incorporates numerous aspects akin to the EU GDPR, this alignment has prefigured Brazil’s endeavours towards obtaining a mutual adequacy finding from the European Commission. In this regard, Brazilian and European Union authorities have been ‘intensively working’ on a mutual-adequacy arrangement for data flows, based on the proximity of the European regulation and the Brazilian law, as explained by the ANPD president Waldemar Gonçalves.

The European Commission is in the process of making “several adequacy decisions” with countries that share similar principles. Brazil is included among these potential partners, and EU Justice Commissioner Didier Reynders ‘plans to travel to the country soon for expected negotiations’. It should be noted that on 22 February 2023, the European Commission issued a Recommendation for a Council decision authorising the opening of negotiations for an agreement between the EU and Brazil on exchanging personal data between Europol and the Brazilian authorities competent for fighting serious crime and terrorism. Regarding a possible GDPR adequacy finding, it is asserted that although the LGPD establishes a robust and extensive

---


117 Available at https://rm.coe.int/t-pd-2022-1rev10-en-final/1680abc6b4

118 ‘Newsroom - Model Contractual Clauses for the Transfer of Personal Data (Module 1)’ (n 116).

119 Available at https://rm.coe.int/t-pd-2023-4rev2-mcc-module-2-en-final/1680ad6a36


124 EDPS Opinion 14/2023 (n 62). In this regard, it is mentioned that unlike Article 6 of Convention 108+, the LGPD does not explicitly classify personal data related to criminal convictions as a special category. Consequently, Brazil lacks a more stringent protective framework for this data, potentially conflicting with the protection standards required by Convention 108+ Parties, such as the European Union (Rosal Santos (n 84)).
data protection framework, there is a need for comprehensive regulations about national security, public security, national defence, and criminal procedure.125

On October 21, 2021, the ANPD announced its incorporation as a voting member within the Ibero-American Data Protection Network (RIPD).126 The RIPD aims to promote the protection of personal data in Latin America by facilitating the sharing of information, experiences, and knowledge among its members. Furthermore, it endeavours to propel regulatory advancements to ensure a progressive and robust framework for safeguarding the right to personal data protection within democratic contexts. The RIPD published, on 20 June 2017, the Standards for Personal Data Protection for Ibero-American States.127 These standards create a unified framework of data protection principles and rights applicable across the various national legislations within the Ibero-American region. On September 27, 2022, the RIPD released the Guide for Implementing Standard Contractual Clauses for International Personal Data Transfers.128 This document outlines specific considerations for conducting international transfers of personal data using SCCs. Notably, the Guide offers guidance for entities conducting data transfers from RIPD member countries to jurisdictions lacking adequate data protection measures.129 This model ‘does not create a binding legal obligation for the Network’s member states to recognise its validity; instead, it offers a view of how national data protection regulators and policymakers in Latin America are collectively approaching the issue of cross-border data transfer tools’.130

Data protection and international law are closely linked by ongoing trade negotiations. These include bilateral and regional deals, and WTO talks, all focused on the digital economy and the vital cross-border data flows for digital commerce. The EU is key in shaping global privacy regulations and safeguarding personal data.131

---

125 Drechsler et al. (n 61).
'From the perspective of the EU, unreservedly committing to free cross-border data flows likely collides with its approach of affording a high level of protection of personal data' as a fundamental right.\textsuperscript{132} In this sense, the EU follows the principle that 'the protection of personal data is non-negotiable'.\textsuperscript{133} Along the same line, the EU's approach is 'to promote its data protection values and facilitate data flows by encouraging convergence of legal systems'.\textsuperscript{134} This implies convergence with the EU's level of data protection, including its data protection principles.

While Brazil is not engaged in significant trade agreements incorporating digital trade provisions, it has shifted its historical defensive stance to better align with the US digital trade agenda.\textsuperscript{135} Given this, Brazil faces the challenge of reconciling the LGPD 'with an ever-increasing alignment with the interests of the United States'.\textsuperscript{136}

At the multilateral level, the Brazilian approach to the Joint Statement Initiative (JSI) on Electronic Commerce, initiated during the WTO 11th Ministerial Conference in December 2017, is worth mentioning. This initiative aims to establish a legally enforceable agreement among its participants, covering conventional trade matters like trade facilitation alongside various digital policy issues such as cross-border data movement, data localisation, online consumer protection, privacy, and network neutrality.\textsuperscript{137}

The JSI has achieved consensus on several policy matters related to enhancing e-commerce. These matters encompassed e-signatures, e-contracts, spam regulation, and paperless trading.\textsuperscript{138} In 2023, negotiations on cross-border data flows faced difficulties, especially on privacy and personal data protection. A partial deal was made on data flows and localisation, with various approaches and proposals under consideration. The latest text showed some agreement among the parties. Some members, led by Australia, Japan and Singapore championed provisions that enable and promote the flow of data,\textsuperscript{139} with limited exceptions to "legitimate public policy objectives",\textsuperscript{140} in line with the US's influence in Asia-Pacific regional trade agreements. However, additional proposals were discussed, such as the European Union's suggestion for an exception related to privacy and personal data protection and Nigeria's proposal for policy flexibility aimed at developing and least-developed countries.\textsuperscript{141} China, for its part, presented its proposal regarding data


\textsuperscript{134} Ibid.


\textsuperscript{136} Wollrad et al. (n 131).


\textsuperscript{140} Ismail (n 138).

\textsuperscript{141} Ibid.
flows, aligning with commitments made in the Regional Comprehensive Economic Partnership (RCEP), expressing support for certain controls over data flows and data localisation requirements.\textsuperscript{142} China has defensive interests ‘in preferring the localisation of servers and public security exceptions for the free flow of data’.\textsuperscript{143} According to the textual proposals on cross-border data flows, it appears that Brazil shared alignment with China in the proposed text concerning cross-border transfers of electronic information, for example, to recognise that each Party “may have its own regulatory requirements concerning the transfer of information by electronic means”.\textsuperscript{144}

At the regional level, the MERCOSUR Agreement on Electronic Commerce, signed on April 29, 2021, is noteworthy. The agreement aims to create a safer environment for the development of e-commerce, benefiting both companies and consumers. It covers several key areas, including the adoption and maintenance of legal frameworks related to the protection of personal data, the free transfer of information by electronic means for commercial purposes, the prohibition of the requirement to install servers in its territory as a requirement for doing business, and the protection against unsolicited commercial messages.\textsuperscript{145} Personal data protection is specifically regulated under Article 6 of the Agreement,\textsuperscript{146} mandating Parties to establish or uphold laws, rules, or administrative measures to protect the personal information of individuals engaged in e-commerce activities, considering global standards. While acknowledging that each Party may have specific requirements concerning electronic information transfer, they are obliged to permit the cross-border exchange of information for commercial purposes via electronic means. Exceptions are allowed if a Party aims to accomplish a valid public policy objective, provided the measure is not arbitrary or unjustifiable, or a covert trade barrier.\textsuperscript{147} Article 8 allows Parties to establish regulations concerning computer facilities, particularly to guarantee the security and privacy of communications. This section also addresses the concept of territoriality, explicitly prohibiting the imposition of a necessity to locate computer facilities within a specific territory as a condition for conducting business. However, there is a recognition that this prohibition might hinder governments from pursuing valid public policy goals. Therefore, despite the clear ban, Parties can impose territoriality requirements as long as these are grounded in legitimate reasons.\textsuperscript{148}


\textsuperscript{148} ibid.
After two decades of talks, the EU and the MERCOSUR states reached a political agreement on 28 June 2019 for a balanced and comprehensive trade agreement. However, the deal is not final yet, as both blocs still need to settle some terms. It is mentioned that the talks were delayed by the EU’s insistence on more environmental safeguards, which prompted Brazil and Argentina to ask for more concessions. The possible trade agreement would include in the Chapter on Trade of Services certain provisions on electronic commerce, related to unsolicited marketing communications and consumer protection. ‘Concerning electronic commerce and personal data protection, the agreement only addresses the prohibition of unsolicited or direct marketing’. Additionally, Article 54, on General Exceptions, states that nothing in the chapter ‘shall be construed to prevent the adoption or enforcement by either Party of measures: [...] (f) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Chapter including those relating to [...] (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts’.

Finally, the Brazil-Chile Free Trade Agreement (FTA) signed in November 2018 included significant commitments regarding the protection of personal information transferred across borders. This agreement specifically aimed at promoting regulatory alignment to ensure consistent levels of personal data protection. Moreover, Chapter 10 of the Chile-Brazil FTA, on Electronic Commerce, acknowledges the importance of safeguarding the “right to the protection of personal data” for users engaged in electronic commerce (Article 10.2.5(f)).

5 Conclusions

Brazil is a relevant global player, leading South-South diplomacy, fostering ties with BRICS countries, and holding significant partnerships with China and the EU. The country holds a prominent position in the digital sphere, standing as Latin America’s largest e-commerce market and an important hub for data centers.

In response to the need for comprehensive data protection regulations, Brazil enacted the LGPD in September 2020. The EU GDPR served as a model for the LGPD, and both laws have many common features. While sharing core aspects with the European regulation, the LGPD also incorporates distinct features tailored to Brazil’s cultural and legal contexts, exemplified by specific provisions like credit protection, indicating potential flexibility in its application.

The LGPD is the cornerstone of Brazil’s data protection framework, presenting a wide-ranging material scope and establishing a comprehensive set of data processing principles, rights and obligations. Following the

152 Lerman et al. (n 147).
154 It should be noted that ‘[w]hile many FTAs are quite benign to privacy, others may be toxic to domestic privacy laws which impose restrictions on cross-border data transfers’ (Graham Greeleaf, ‘Looming Free Trade Agreements Pose Threats to Privacy’ (2018) 152 Privacy Laws & Business International Report, 23-27, UNSW Law Research Paper No. 18-38).
GDPR’s approach, the LGPD has a broad extraterritorial reach. The Brazilian Data Protection Authority, the ANPD, plays a crucial role ensuring compliance with LGPD provisions.

Chapter V of the LGPD regulates the cross-border transfer of personal data. These provisions allow personal data transfers if the destination country maintains an adequate level of protection, which the ANPD assesses. Furthermore, the LGPD allows international data transfers under specific circumstances. This includes scenarios where the data controller assures the safeguarding of personal data through distinct means: via transfer-specific contractual clauses; adherence to SCCs; compliance with binding corporate rules; or through seals, certificates and codes of conduct regularly issued. In addition, cross-border transfers are permitted when: it is necessary for international legal cooperation between government intelligence, investigations, and prosecution authorities; it is authorised by the ANPD; it is necessary for public policies or public service activities; data subjects have provided specific and highlighted consent for the transfer upon prior information; it is necessary for the fulfilment of a legal or regulatory obligation on the part of the controller; it is for a contract or procedures related to a contract in which the data subject is a party, as required by the data subject himself; and it is for the regular exercise of rights, including contractual performance and in court, administrative, or arbitration proceedings.

ANPD released on August 15, 2023, a draft regulation on data transfers, which sets the requirements and guarantees for personal data exports, defines the content of SCCs, outlines the analysis process for specific contractual clauses and binding corporate rules, and specify the adequacy decision assessment process for the data protection equivalence of foreign countries or international organizations. The draft outlines procedures for ANPD's recognition of equivalence for standard contractual clauses from other countries or international organisations (a process that may be initiated ex officio or upon the request of the interested parties), emphasising approval prioritisation for widely applicable clauses. It also proposes a template for SCCs.

Brazil is currently seeking mutual adequacy recognition from the European Commission. The country has also expressed interest in potentially joining Convention 108+. As Brazil engages in ongoing trade negotiations and participates in multilateral forums like the WTO, it faces challenges in reconciling its LGPD with multiple digital trade interests.

It can be argued that SCCs are key instruments for ensuring compliance with the Brazilian data protection framework when transferring personal data internationally. SCCs standardize the data protection obligations of data exporters and importers, regardless of the adequacy status of the destination country. The ANPD draft regulation on data transfers highlights the importance of SCCs in enhancing data transfer mechanisms, as well as the ANPD’s role in assessing and approving them, reinforcing the accountability measures for all parties involved in the data transfer process.

To foster convergence of data protection standards, it could be beneficial to align the Brazilian SCCs models, as much as possible, with the RIPD’s SCCs approach. Moreover, if Brazil joins Convention 108+, it should also ensure compatibility with the Committee of Convention 108 Model Contractual Clauses for transborder data flows of personal data.

Brazil could also take a proactive stance in promoting the use of SCCs at the international level, as a mechanism that fosters interoperability between different legal frameworks for protecting privacy and personal data. This could include adopting and mutually recognizing, where appropriate, similar SCCs that adhere to high standards of personal data protection.

Acknowledgement: This research has been funded by Cerre, Brussels, Belgium