Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What Brazil's Adequacy Status Will Mean For EU Data Flow

By **Ahmed Baladi, Vera Lukic and Hermine Hubert** (March 10, 2026, 3:01 PM GMT)


Ahmed Baladi


Vera Lukic


Hermine Hubert

On Jan. 26, the European Commission adopted an implementing decision formally recognizing Brazil as providing an adequate level of protection for personal data transferred from the European Union.[1]

This historic decision makes Brazil the third Latin American country to secure full adequacy status, following Argentina in 2003 and Uruguay in 2012, and positions Brazil as a major gateway for EU-Latin America data flows.

This decision forms part of a mutual adequacy agreement whereby Brazil has also recognized the EU as offering adequate data protection standards, allowing businesses, public authorities and researchers to freely exchange data between the EU and Brazil.

This article examines in particular the commission's adequacy decision, situating Brazil's achievement within the broader global landscape of cross-border data transfer frameworks.

It addresses the key findings underlying the commission's assessment, compares Brazil's position with other recognized jurisdictions, both within Latin America and beyond, and provides practical guidance for organizations navigating international data transfers in light of these developments.

Why Brazil Made the Cut

The commission's adequacy finding is grounded in a comprehensive analysis of Brazil's legal framework, covering both the rules applicable to private-sector data importers, and the limitations and safeguards governing public authorities' access to personal data. Under the General Data Protection Regulation, the commission must determine whether a third country guarantees a level of protection essentially equivalent to that ensured within the EU.[2]

Crucially, however, the Court of Justice of the EU has clarified that third countries need not ensure protection identical to that guaranteed under EU law. What matters is whether, in practice, the foreign system as a whole delivers the required level of protection through effective rights, safeguards and enforcement mechanisms.[3]

Brazil's framework satisfied these requirements through several pillars. First, privacy and data protection are enshrined as fundamental rights in Brazil's Federal Constitution, with Article 5 protecting intimacy and private life, guaranteeing the secrecy of correspondence and communications and, following Constitutional Amendment No. 115 of February 2022, establishing an explicit right to the protection of personal data both online and offline.

Second, Brazil's General Data Protection Law, Lei Geral de Proteção de Dados, or LGPD,[4] enacted in 2018, provides comprehensive safeguards for all individuals, regardless of nationality.

The LGPD's structure and main components closely mirror those of the GDPR. It establishes principles of lawfulness, purpose limitation, data minimization, accuracy, storage limitation and security in terms substantially similar to Articles 5 and 6 of the GDPR.

It requires controllers and processors to rely on specified legal bases for processing, including consent, contractual necessity, legal obligation, legitimate interests and others, and imposes heightened conditions for the processing of sensitive personal data. Data subject rights under the LGPD, including rights of access, rectification, deletion and portability and rights related to automated decision-making, parallel those under the GDPR.

Brazil's institutional framework also played a critical role in the commission's assessment. The National Data Protection Authority, Agência Nacional de Proteção de Dados, or ANPD, was created by the LGPD in 2018, and was transformed into an independent authority of "special nature" in 2022, enjoying technical and decision-making autonomy with its own assets and budget.

In September last year, the ANPD obtained its agency status, bringing its independence in line with Brazil's other regulatory agencies, such as those overseeing electricity and telecommunications. The ANPD has comprehensive investigatory and enforcement powers, including the authority to conduct audits, request information, impose warnings and fines, and order processing activities to cease.

On government access, the commission found that Brazilian law imposes significant limitations on law enforcement and national security agencies seeking access to personal data, with prior judicial authorization required in most cases.

The Brazilian Supreme Court's landmark 2020 ruling recognizing data protection as a fundamental right, combined with the LGPD's application to public authorities, including for intelligence purposes, further reinforced the commission's confidence that Brazil offers adequate safeguards against disproportionate government access to personal data.[5]

Context: Brazil Joins an Exclusive Club

Brazil's adequacy status is particularly significant when viewed against the backdrop of Latin America's data protection landscape. Until now, Argentina and Uruguay were the only Latin American jurisdictions with full EU adequacy recognition, having received their decisions in 2003 and 2012, respectively.

Brazil's entry brings the total number of adequacy-recognized Latin American countries to three, a notable expansion given the region's growing importance in global data flows.

The European Commission's decision positions Brazil as a regional leader in data protection governance. Notably, Brazil has achieved this level of adequacy under the GDPR framework, which imposes a higher

compliance threshold than its predecessor, Directive 95/46/EC.

Several factors contributed to this achievement that other Latin American nations have not yet adopted. Brazil enshrined data protection as a fundamental right in 2022, and Brazil's ANPD has demonstrated active enforcement, issuing sanctions against both private companies and public authorities.

Brazil's adherence to the American Convention on Human Rights and recognition of the Inter-American Court of Human Rights' jurisdiction provide additional layers of judicial protection. Other Latin American jurisdictions seeking adequacy will need to match this combination of constitutional protection, comprehensive legislation, independent supervision and demonstrable enforcement.

In recent years, countries such as Mexico, Chile and Peru have undertaken significant reforms of their data protection laws, but none have yet achieved the institutional maturity or enforcement track record that the commission found in Brazil.

Global Adequacy Landscape

Globally, the commission has adopted adequacy decisions for a relatively select group of jurisdictions. These include Andorra, Argentina, Canada, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the U.K., Uruguay and the U.S., under the EU-U.S. Data Privacy Framework. Brazil now joins this list.

Notably, many economically significant jurisdictions remain without adequacy status. India, despite enacting its Digital Personal Data Protection Act in 2023, has not received adequacy recognition. Asia-Pacific economies, including Australia, New-Zealand, Singapore, Thailand and Vietnam similarly lack adequacy decisions, notwithstanding growing data protection maturity.

Brazil's achievement is therefore both a validation of its legislative and institutional progress and a potential model for other countries seeking to facilitate data flows with Europe.

Implications for International Data Transfers

The practical effect of the adequacy decision is straightforward. Personal data may now flow from EU-based controllers and processors to recipients in Brazil without the need for appropriate safeguards, such as standard contractual clauses or binding corporate rules, or other transfer mechanisms allowed under the GDPR. Likewise, transfer impact assessments and potential supplementary measures need not be conducted on a case-by-case basis, following the Schrems II CJEU ruling in 2020.[6]

Accordingly, the decision removes a significant compliance burden for organizations with EU-Brazil data flows.

This streamlined transfer regime applies to all data transfers falling within the LGPD's scope. Importantly, however, the decision does not affect the direct applicability of the GDPR to Brazilian entities where the conditions laid down in Article 3 of the GDPR are met, for example, where a Brazilian company offers goods or services to individuals in the EU or monitors their behavior.

The adequacy finding also has implications for onward transfers from Brazil. The LGPD contains its own international transfer framework, requiring adequacy decisions, standard contractual clauses, binding corporate rules or other approved mechanisms for onward transfers to third countries.

The continuity of protection requirement ensures that personal data originally transferred from the EU does not lose its protection when subsequently transferred from Brazil to a third jurisdiction.

Business Implications

For multinational corporations, the adequacy decision simplifies operational compliance in several respects. Organizations previously relying on standard contractual clauses for EU-to-Brazil transfers now eliminate the administrative burden associated with signing contractual clauses, record-keeping and transfer impact assessments specific to those transfers.

Intragroup data sharing, e.g., for centralized human resources systems, customer relationship management or global IT infrastructure hosted in Brazil, no longer requires the layered documentation that standard contractual clauses or binding corporate rules demand.

The decision may also influence corporate decisions regarding data center and processing location. Brazil's combination of adequacy status, Portuguese and Spanish language capabilities, time zone compatibility with both European and U.S. business hours, and a large domestic technology sector makes it an increasingly attractive hub for regional data processing operations.

Companies serving both European and Latin American markets may now consider consolidating processing activities in Brazil without fragmenting data flows.

However, adequacy should not be considered as a complete substitute for due diligence. Adequacy simplifies the lawfulness of the transfer itself, but it does not eliminate obligations around data security, breach notification, data subject rights or other GDPR requirements that apply to the exporting controller.

Finally, businesses should note that the commission's decision includes a monitoring mechanism, with a first review scheduled within four years and periodic reviews thereafter.

The decision can be suspended, repealed or amended if adequate protection is no longer ensured, as demonstrated by the commission's invalidation of prior adequacy mechanisms for the U.S. following the Schrems I and Schrems II rulings of the CJEU in 2015 and 2020, respectively.[7]

Key Takeaways

The adequacy decision marks a significant milestone for EU-Brazil data flows. For organizations currently navigating the complexity of standard contractual clauses or binding corporate rules, this decision offers a meaningful opportunity to simplify transfer mechanisms and reduce compliance overhead.

But simplification should not be mistaken for a compliance exemption. The adequacy finding removes transfer-specific barriers, it does not suspend the GDPR's core requirements. Organizations should continue to ensure a valid legal basis for processing, implement appropriate security measures, adhere to data minimization principles and formalize processor relationships through compliant agreements.

Privacy policies and records of processing activities should also be updated accordingly. Besides, data protection authorities retain their full enforcement powers and individuals maintain their rights to lodge complaints.

Equally important is the reality that adequacy is not permanent. Developments in Brazilian data protection law and ANPD enforcement activity that could affect the decision's continued validity should be carefully monitored.

Any concerns identified during the commission's first review, expected in 2030, may affect the decision's scope or validity. Therefore, ANPD guidance, decisions and any legislative developments that could alter the adequacy analysis should be closely followed.

In light of these considerations, organizations should take advantage of the compliance efficiencies this decision provides, while remaining attentive to Brazilian regulatory developments. Those that strike this balance will be best positioned to realize the full benefits of the EU-Brazil adequacy framework for years to come.

Ahmed Baladi and Vera Lukic are partners, and Hermine Hubert is an associate, at Gibson Dunn & Crutcher LLP.

[1] https://ec.europa.eu/commission/presscorner/detail/en/ip_26_229.

[2] Recital 104 of the GDPR.

[3] CJEU, Case C-362/14, Schrems, paragraphs 74 and 75.

[4] https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf.

[5] https://edpl.lexxion.eu/article/EDPL/2020/4/21.

[6] CJEU, Case C-311/18, Schrems II. Controllers or processors are responsible for verifying, on a case-by-case basis, whether the law or practice of the non-EEA country impinges, for example due to legislation imposing access to data, on the effectiveness of the appropriate safeguards contained in the Art. 46 GDPR transfer tools.

[7] Case C-362/14, Schrems ('Schrems I') and Case C-311/18, Facebook Ireland and Schrems ('Schrems II').