

How US Cos. Should Prep For Brazil's Int'l Data Transfer Rules

By **Juliane Chaves Ferreira** (July 23, 2025, 5:42 PM EDT)

On Aug. 23, Brazil's National Data Protection Authority, or ANPD, will begin enforcing mandatory standard contractual clauses for international data transfers.

This change, introduced by Resolution CD/ANPD No. 19, directly affects any foreign company, including U.S.-based businesses, that processes or stores the personal data of individuals in Brazil.

In a global economy where cross-border data flows are essential to digital services, cloud computing, e-commerce and software-as-a-service operations, understanding and complying with these requirements is critical.

While the regulatory framework is inspired by the European Union's General Data Protection Regulation, it brings unique obligations and deadlines for businesses engaging with the Brazilian market.



Juliane Chaves
Ferreira

New Requirements for Cross-Border Data Transfers in Brazil

On Aug. 23, 2024, the National Data Protection Authority published the resolution approving the regulation on the international transfer of personal data, including the content of the standard contractual clauses, which must be incorporated into existing contracts and establish a data protection regime considered adequate, even in countries with different data protection laws.

The standard contractual clauses can be found in Annex II of Resolution CD/ANPD No. 19. The ANPD established that the mandatory implementation of standard contractual clauses in contracts must occur without modifications — 12 months after publication — by Aug. 23, 2025.

In a context in which digital commerce occupies a central role in the global economy, the international transfer of data has become an essential practice for the operation and scalability of businesses, which is why it is essential that companies comply with the regulatory body's most recent guidelines and be aware of the final deadline for adapting their operations.

With the new regulation, the ANPD sought to harmonize the level of data protection in the international context, ensuring that the circulation of personal information between different countries occurs in a secure manner and is compatible with the standards established by the General Data Protection Law, or LGPD.

To this end, the regulation also brought clear definitions on the characteristics of an international data transfer.

What Constitutes an International Data Transfer?

In this sense, the legislation clearly defines the roles of the exporter and importer of personal data, as the processing agent that transfers personal data to an agent located in a foreign country or international organization, and the international agent that receives such personal

data, respectively.

It is important to emphasize that the collection of international data should not be confused with the activity of international data transfer. While the former deals with the direct collection of data by the processing agent of a foreign country or international organization, the latter occurs between controllers and presupposes some level of data processing in the national territory and its subsequent transmission abroad.

It will be up to the controller to assess, based on the circumstances of the specific case, whether a given operation constitutes an international transfer under the terms of the regulation.

In line with the ANPD resolution, an international transfer of data is considered to be the sending of personal data to a foreign country or to an international organization of which Brazil is a member.

Examples Relevant to U.S. Companies

In this sense, an e-commerce company headquartered in Brazil that uses a cloud storage service with servers located in the U.S. would be an example of an international transfer.

If this cloud service is provided by a U.S. company such as Amazon Web Services, Google Cloud or Microsoft Azure, it will fall under the scope of the standard contractual clause requirement. When recording personal information of Brazilian customers, such as names, addresses and payment details, the data is transmitted directly abroad.

The same reasoning applies to transfers made between companies belonging to the same multinational economic group. A U.S.-based multinational that shares data between its Brazilian subsidiary and its American headquarters will be required to comply with the new rules, even if all entities are under the same corporate control. The movement of data between entities located in different jurisdictions constitutes an international data transfer activity.

To ensure the legality and security of these operations, the ANPD establishes specific mechanisms, one of which is geographic approval of assessment, in which the authority can recognize and publicize, through its own procedures, a given country or international organization that ensures a level of personal data protection compatible with that provided for in the LGPD.

How Brazil's Approach Compares to GDPR and California Privacy Rights Act

Similar to the EU's GDPR, Brazil's LGPD establishes a framework to ensure that personal data transferred abroad receives adequate protection. For U.S. companies already subject to the GDPR or the California Privacy Rights Act, many of the concepts will feel familiar, but the specific contractual obligations and deadlines in Brazil require targeted legal and operational adjustments.

The publication of Resolution No. 19 signals the ANPD's commitment to building a secure and interoperable digital ecosystem. To date, no country has been recognized by the ANPD, but it is expected that in the coming years the authority will move forward with new recognitions of countries with an adequate level of protection and promote international agreements that facilitate the flow of data between jurisdictions, especially with strategic markets such as the EU, the U.S. and Latin American countries.

The Role of Standard Contractual Clauses

The second aspect of international data transfers occurs when the controller offers and proves guarantees that the principles, rights of data subjects and the data protection regime provided for in the Brazilian legislation will be respected in the destination country.

These guarantees can be formalized through the adoption of specific contractual clauses or through standard contractual clauses approved by the ANPD.

Standard contractual clauses function as legal instruments previously approved by the ANPD to ensure that personal data transferred outside Brazil continues to receive a level of protection compatible with the principles and rights provided for in the LGPD.

They must be incorporated into contracts entered into between the data exporter and the data importer, regardless of whether they belong to the same economic group. This is particularly relevant for U.S. companies that outsource processing services or rely on cross-border data sharing with Brazilian entities. The adoption of standard contractual clauses eliminates the need for prior authorization from the ANPD, as long as they are used in full without changes to their essential content, which provides greater agility and legal predictability to international data processing operations.

The structure adopted by the ANPD is similar to the European model, especially with the use of standard contractual clauses. As is the case with the GDPR, Brazil now requires that data transfers to countries without an adequacy decision be supported by robust contractual instruments.

This regulatory convergence facilitates the operations of multinational companies and reinforces Brazil's credibility as a reliable business partner in terms of data protection.

Deadline and Compliance Risks for U.S. Businesses

According to Resolution No. 19, the mandatory adoption of standard contractual clauses comes into effect on Aug. 23, exactly one year after the publication of Resolution CD/ANPD No. 19, which deals with the matter.

Until then, organizations that carry out international data transfers must review their data flows, identify the destinations involved and evaluate the mechanisms currently used to ensure compliance with the LGPD.

If they do not adopt another valid mechanism — such as adequacy decisions or specific clauses approved by the ANPD, which require prior approval — the standard contractual clauses must be incorporated into the applicable international contracts. It is recommended that companies begin this process of reviewing and adapting their contracts now, in order to avoid regulatory risks, ensure legal certainty and maintain the continuity of international operations that depend on the flow of personal data.

Failure to adopt valid mechanisms for international transfers may subject the controller to the administrative sanctions provided for in the LGPD, including warnings, fines and publicity of the violation. In addition, there are significant reputational risks, especially for U.S.-based companies in sectors such as e-commerce, financial services, education and health, which often process large volumes of personal data from Brazilian users.

Therefore, it is recommended that companies assess the need to adopt the measures imposed by the ANPD within the established deadline, so that they continue to operate in compliance in Brazil.

Juliane Chaves Ferreira is an associate attorney at Guimaraes & Vieira de Mello Advogados.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.