Brazil Court Reminds Businesses of Key Data Protection Obligations – What Do Those Doing Business in Brazil Need to Know?

Insights
11.06.24

Four years after the Brazilian General Data Protection Law (LGPD) came into force, Brazil's Superior Court of Justice (STJ) recently issued a list of precedents exploring how the court applied the law and addressed the changes introduced by it. These cases offer helpful data privacy guidance to businesses based in and doing business in Brazil. What are the key precedents and what do businesses need to know to stay compliant?

Quick Background

The LGPD came into effect in 2020 and applies to personal data, which is defined as "information regarding an identified or identifiable natural person." It lays out the rules on data processing, ensuring appropriate security of personal data, including protection against unauthorized or unlawful processing and against accidental loss. The LGPD establishes the principles and legal grounds for data processing in Brazil, the data subjects' rights, the processing agents' obligations, and the sanctions and fines for noncompliance.

6 Precedents You Need to Know About

The following cases were listed by the Superior Court of Justice as precedents on the LGPD application:

1. Automated data analysis is subject to the LGPD. In 2024, the STJ determined that data analyzed in the process of cancelling service providers' registration, such as gig economy drivers, is personal data and therefore subject to the LGPD. This decision originated from a claim by a driver who argued he was removed from a platform but not properly notified about the decision. He claimed this action violated his right to defense and due process. The reporting justice noted that the removal resulted from an automated analysis. Because the LGPD ensures the data subjects' rights to not only request the revision of automated decisions that impact their professional profiles but also access clear information on the treatment of their personal data, the STJ ruled in the driver's favor. The court ruled that the driver had to be informed about the reason for the cancellation and had the right to request a review of the decision under the LGPD. *[Proceeding REsp 2.135.783]*

2. Data leaking does not automatically confer indemnification right to the data subject. In 2023, the Superior Court of Justice determined that, although data leaking is an undesirable failure, it does not by itself result in the right to indemnification by the data subject. This decision originated from a claim by a data subject who sought indemnification for damages against a local energy utility company after it leaked her personal data and caused undue access by third parties. The court stated that the data leaked was not sensitive data and, therefore, is not afforded special protection by the LGPD. As a result, the access to non-sensitive data by third parties does not automatically confer the data subject the right to indemnification for damages. The court said parties need to prove actual harm resulting from such access in order to succeed on their claims. *[Proceeding AREsp 2.130.619]*

3. Brazil Stock Exchange must remove unauthorized investors' data. In 2023, the STJ ordered Brazil Stock Exchange to remove investors' registration data unduly included by third parties who had non-authorized access to the investors' profiles. In this case, third parties accessed and edited the investors' data through a fake account created in a brokerage firm. In its defense, Brazil Stock Exchange argued that the fraud took place externally, in an associated brokerage firm. However, the STJ responded that, by creating a system to store investors' data, Brazil Stock Exchange is treating personal data. Therefore, it is bound to the LGPD's rules on the matter and must observe its safety requirements. The court ordered it to remove and correct existing personal data when required by the data subject. *[Proceeding Resp 2.092.096]*

4. Financial institution is responsible for undue treatment of data used in a scam. In 2023, the STJ determined that a financial institution is liable for a flawed data treatment when such data is accessed and used by a fraudster to carry out a scam. In this case, a client of a financial institution had her debt data accessed by a fraudster, who used it to carry out a scam and steal money from the client. The court ruled that the financial institution provided a faulty service under the LGPD by improperly storing data and allowing third parties to access confidential information, causing damage to consumers. Therefore, the STJ held the financial institution responsible for repairing the damage caused to the consumer. *[Proceeding Resp 2.077.278]*

5. Validity of the delivery of personal information by public officials. In 2022, the STJ confirmed the validity of a Decree that requires public officials to annually turn over information on their personal assets. This decision originated from a claim by the Union of Tax Auditors of Minas Gerais against the state of Minas Gerais, questioning the legality of the Decree. While the Union argued that this requirement violates the constitutional right to privacy and intimacy, the court replied that these rights are not absolute and that public officials are subject to reduced privacy and intimacy. The court also stated that the government has a legal duty of protecting the information handed by the public officials, adopting the measures required by Brazil Federal Constitution and the LGPD. *[Proceeding RMS 55.819]*

6. Internet service providers must provide data of users that post videos offending the memory of deceased people. In 2021, the STJ determined that internet service providers must hand in registration data (such as name, ID, and taxpayer number) belonging to users that post videos

offending the memory of a deceased person. This decision was raised in a lawsuit initiated by the family of a deceased Brazilian politician, seeking to obtain data of users that posted videos online offending her memory and asking the removal of the videos. The STJ has long held that courts can intervene to obtain protected data in situations where this data is needed to instruct judicial proceedings. The court also stated that the LGPD does not rule out the possibility of breach of secrecy. Rather, it establishes rules for doing so. *[Proceeding REsp 1.914.596]*

What Does This Mean to Employers Doing Business in Brazil?

The precedents above show that Brazilian courts are carefully revising matters involving personal data and rigorously enforcing the LGPD. Adhering to the LGPD is crucial for U.S. companies doing business in Brazil. Ensuring compliance mitigates legal risks, avoids the payment of significant fines, and enhances your company's reputation for respecting data privacy.

Remember that breaches of the LGPD may result in administrative sanctions that range from a simple warning to the partial or full suspension or prohibition of the activities related to the noncompliant data processing. There may also be the application of fines: simple fines of up to 2% of a company's revenue in Brazil for the prior financial year, up to a total maximum of $50 million Brazilian Reais (approximately $8.7 million USD) per infraction, as well as daily fines, limited to the same maximum as the simple fines.

What Should Your Business Do?

As we previously reported, if you think the LGPD may apply to your business, work with experienced counsel to ensure that you are compliant with its requirements. To stay compliant, you should take at least the following measures:

- Develop and implement a data privacy policy compliant with the LGPD;
- Review and update your agreements with clients, contractors, and employees to ensure compliance with the LGPD;
- Map and register the personal data that is being processed;
- Assess the need to hire a Data Protection Officer; and
- Ensure that agreements involving international data transfers contain the standard contractual clause, or that you have authorization to use specific contractual clauses or a global corporate rule. If you are a data controller, ensure that you have implemented transparency measures.

Conclusion

If you require any assistance related to data protection compliance in Brazil, please contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our International Practice Group. We will continue to monitor the situation and provide updates as warranted, so you should

ensure you are signed up for the Fisher Phillips Insight System to receive the most up-to-date information.

Related People

Meilin Ng Canova
Visiting Legal Professional
610.230.2181
Email

Service Focus

International

Privacy and Cyber