




TozziniFreire.

Cybernews

7th Edition | 2025

This is an informative newsletter
produced by the **Cybersecurity & Data Privacy**
practice of TozziniFreire Advogados.

INDEX

Click at the topic of your
interest and browse
through the content 

01 EDITORIAL

02 GENERAL NEWS

One year since Resolution No. 19/2024 has been published: what are the possible scenarios for international data transfers?

CNJ System exposed data related to Pix keys of 11 million people

Credit score banks cannot provide data to third parties, as ruled by STJ

TJMG orders credit agency to indemnify consumer for violation of LGPD

EDITORIAL

In this edition of the Cybernews Newsletter, we highlight the main news on data protection in August 2025.

Firstly, we analyze the scenario one year after Resolution No.19/2024 has been published. In addition, we announced that the CNJ (National Council of Justice) reported the leak of data linked to the PIX keys of 11 million users, as a result of unauthorized access by third parties to the Judiciary Branch's Assets Search System (Sisbajud).

Moreover, the Superior Court of Justice (STJ in Portuguese) ruled that credit databases cannot share consumers' personal information without consent. The STJ ordered the defendant to pay BRL 11,000 as moral damages and to refrain from sharing the plaintiff's data without prior authorization, except for other databases. The recent ruling by STJ reinforces a new paradigm for data management in Brazil, emphasizing that unauthorized data sharing results in moral damages claims.

Finally, the Court of Justice of Minas Gerais (TJMG in Portuguese) ordered a credit protection agency to indemnify a consumer in BRL 10,000 reais for pain and suffering, after the improper sharing of his personal data, in violation of LGPD. The decision recognized a failure in information security and highlighted the consumer's vulnerability in the face of the company's economic power, also applying the principles of the Consumer Protection Code. The case reinforces the importance of data protection and the responsibility of companies in processing this information.

GENERAL NEWS

One year since Resolution No. 19/2024 has been published: what are the possible scenarios for international data transfers?

August marks two important moments for data protection in Brazil: the seven-year anniversary of the publication of LGPD (Law No. 13,709/18) and the first anniversary of Resolution No. 19/2024, from ANPD (Brazilian Data Protection Authority). The latter consolidated rules on the international transfer of personal data — a topic of great practical relevance that requires the adoption of various measures in light of the globalization of operations.

Published in August 2024, Resolution No. 19 presented detailed definitions of certain mechanisms currently available for the international transfer of personal data, reaffirming the formal and material requirements applicable to each.

Among the mechanisms provided, the Standard Contractual Clauses (SCCs), approved as an annex to the Resolution, stand out. These consist of provisions that can be used to enable international transfers. In the current scenario, the adoption of SCCs

has proven to be the most feasible measure for most data processing agents in Brazil, particularly for companies that do not wish to create customized mechanisms or that need to quickly demonstrate compliance.

In this context, the Resolution established a 12-month deadline from its publication date for companies opting for this mechanism to incorporate SCCs. Such deadline will end on August 23, 2025, so it is essential for companies to comply with the necessary requirements to avoid sanctions and penalties.

In addition to SCCs, an alternative mechanism is the submission of specific contractual clauses for ANPD's analysis. Such mechanism allows the parties to draft clauses tailored to the specifics of their operations, which can be useful for organizations with more complex flows or those that already have ongoing international agreements. However, ANPD's individual analysis may require time and resources for drafting, thus requiring planning by the interested companies.

Another mechanism provided is the Binding Corporate Rules (BCRs), aimed specifically at multinational corporate groups. Despite being recognized as robust governance instruments, ANPD has not yet published approvals of BCRs in Brazil. The process tends to be slower due to the complexity and level of detail required, which may have discouraged the use of this mechanism thus far.

Finally, the Resolution also addresses the so-called adequacy decisions, recognizing that certain countries or international organizations offer a level of personal data protection equivalent to that provided for in LGPD. This is one of the most efficient mechanisms for facilitating transfers, as it eliminates the need for additional instruments. Despite expectations for the

European Union to recognize it by the end of 2025, ANPD has not published any adequacy decisions yet.

Conclusion

SCCs have proven to be the most accessible and legally secure mechanism to facilitate international transfers of personal data at this moment, especially given the absence of adequacy decisions and the complexity involved in the approval of other instruments. For the adoption of such mechanism, and considering the current regulatory deadline, companies are expected to be already at an advanced stage of contractual review and adaptation of their data flows, in order to ensure compliance in light of the deadline that ends on August 23, 2025.



CNJ System exposed data related to Pix keys of 11 million people

The Central Bank (BC) and the National Council of Justice (CNJ) reported a security incident involving unauthorized access to the Judiciary Branch's Asset Search System (Sisbajud) operated by CNJ, relating to personal data linked to Pix keys.

According to CNJ, the incident resulted in unauthorized access to registration information of more than 11 million people, approximately 7% of individuals with a Pix key.

In addition, the individuals' name, bank name, branch number, and account number were also accessed, although the Council stated that there was no access to any data protected by bank secrecy, such as balances, passwords, or statements, nor access to deposited amounts.

CNJ said it will not use other means of communication with those affected, such as messages, SMS, email, or phone calls.

This event underscores the importance of continuously monitoring personal data handling practices and of implementing strict policies that ensure information security, along with measures of transparency and accountability from institutions.



Credit score banks cannot provide data to third parties, as ruled by STJ

The Superior Court of Justice (STJ in Portuguese) ruled that credit database managers cannot share consumers' personal information without proper authorization. This decision was reached after a special appeal was filed by an individual whose data, such as monthly income and address, was disclosed without his consent by a credit scoring company.

The individual sought not only to prohibit his data from being disclosed but also filed a claim for moral damages. While São Paulo Court of Justice (TJSP) had deemed the claim groundless, arguing that the data was kept for credit protection and was not sensitive information, the 3rd Chamber of STJ ruled differently.

Reported by justice Nancy Andrighi, the decision ordered the company to pay BRL 11,000 in moral damages and refrain from sharing the plaintiff's data with third parties without prior authorization, except for other databases which are permitted to share such data. The justice emphasized that this practice causes pain and suffering and should be avoided, citing STJ precedents to support the decision.

The recent ruling by STJ reinforces a new paradigm for the data management sector in Brazil, where unauthorized data sharing results in moral damages claims.



TJMG orders credit agency to indemnify consumer for violation of LGPD

The 13th Civil Chamber of Minas Gerais Court of Justice ordered a credit protection agency to pay BRL 10,000 as moral damages due to the improper sharing of a consumer's personal data, in violation of LGPD.

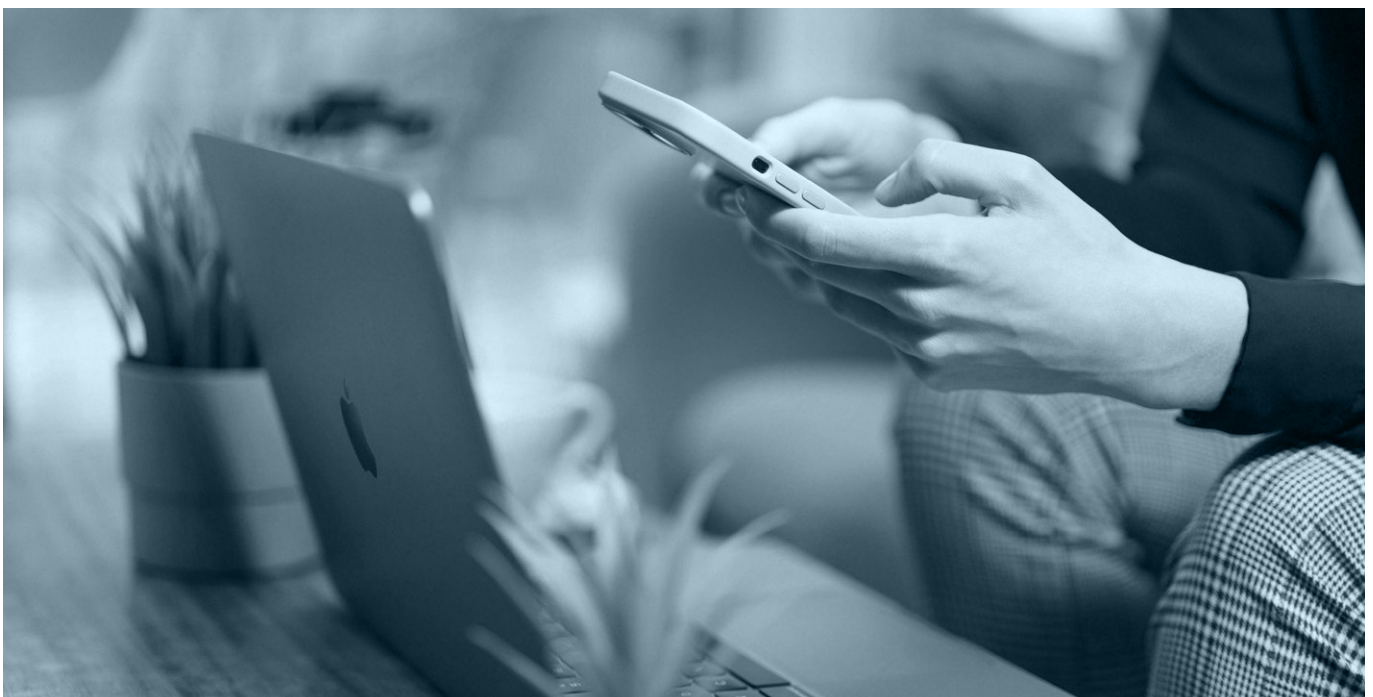
The consumer discovered, by means of a certification issued by the company, that his information was improperly disclosed in 2020 and 2021. In a lawsuit, he sought to stop the sharing of his data and requested BRL 20,000 in compensation.

Although the request was denied in the lower court, appellate judge Newton Teixeira Carvalho, upon reviewing the appeal, acknowledged the violation of LGPD and emphasized the lack of security in data

protection: "An institution that does not employ sufficient security to prevent data leaks is non-compliant with LGPD, violating its provisions."

The appellate judge also highlighted the consumer's vulnerability in relation to the company, reinforcing the need for direct compensation to him, as per the Consumer Protection Code (CDC). Thus, the court upheld the decision, resulting in the award of BRL 10,000.

This case serves as a warning to companies about the importance of LGPD and the need for robust security measures to prevent civil injuries.





Partners responsible for the newsletter

- ⑧ Patrícia Helena Marta Martins
- ⑧ Marcela Waksman Ejnisman
- ⑧ Carla do Couto Hellu Battilana
- ⑧ Luiza Sato
- ⑧ Bruna Borghi Tomé
- ⑧ Sofia Kilmar
- ⑧ Stephanie Consonni de Schryver