LGPD AND FINANCIAL SECTOR LEGISLATION

campos thomaz
& meirelles advogados

1

GENERAL DATA PROTECTION LAW

Law No. 13,709/2018 ("General Data Protection Law" or "LGPD") establishes rules and guidelines for the processing of personal data, both in the virtual and physical environment in the public and private spheres. Its main objective is to guarantee the protection of the privacy and fundamental rights of the holders of this information[1].

In general terms, the LGPD determines that:

Processing agents must record processing operations involving personal data, especially based on the legal basis of legitimate interest

Controllers must provide a communication channel so that data subjects can exercise their rights under the LGPD

Data processing must be carried out by one of the legal bases provided for in the LGPD

Organizations must comply with data subject rights, such as access, rectification, deletion, and others

The controller must prepare a Personal Data Protection Impact Report ("RIPD") to assess the risks involved in the processing of personal data

Inform the criteria and procedures used in automated decision-making by the controller, observing commercial and industrial secrets

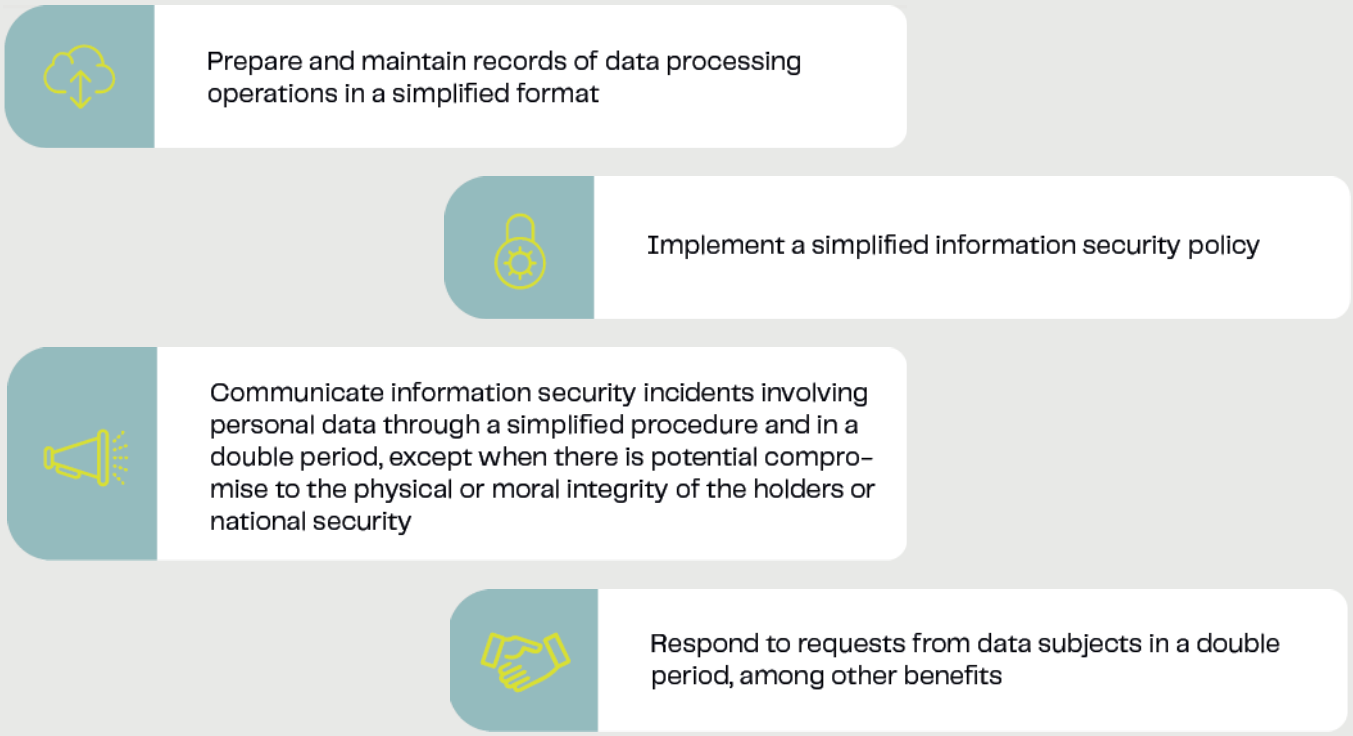
Communicate to the ANPD and the data subjects in the event of an information security incident involving personal data that may generate risk or relevant damage to the data subjects

Adopt security, technical, and administrative measures to protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication, or any form of illegal or inappropriate treatment

[1] Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. It was accessed on 16 March 2023.

1.1 CD/ANPD Resolution No. 2/2022

Resolution CD/ANPD nº 2/2022[2] approved the regulation for applying the LGPD, bringing flexibility and more favorable aspects to business development for small treatment agents, as defined in Article 2, Item I[3]. Among the flexibilities provided for in the resolution, small agents can:



In this regard, fintech must conduct a diligent and cautious assessment of the resolution, given that general and specific criteria determine the planned flexibility's non-applicability[4].

1.2 Cyber Security

Resolution of the Conselho Monetário Nacional ("CMN") No. 4,893/2021[5] and Resolution of the Banco Central ("Bacen") No. 85/2021[6], establish guidelines on the cybersecurity policy, action plan, and response to incidents, in addition to of requirements for contracting cloud processing and storage services. Fintechs must observe such regulations and payment institutions ("IPs") authorized to operate by Bacen.

It is worth mentioning that although IPs are considered fintechs, they are not subject to the rules determined by Resolution No. 4,893/2021. Instead, IPs must follow the provisions outlined in Resolution No. 85/2021 when they receive authorization from BACEN to operate.

[2] Available at: < https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. It was accessed on 16 March 2023.
[3] CD/ANPD Resolution No. 2/2022, Art. 2, inc. I. Small-sized processing agents: micro-companies, small-sized companies, startups, legal entities governed by private law, including non-profit entities, under the terms of current legislation, as well as natural persons and depersonalized private entities that process personal data, assuming typical controller or operator obligations.
Such as the processing of personal data that may significantly affect the interests and fundamental rights of the holders (e.g., financial fraud or identity theft) and the processing of personal data in the context of decisions taken solely based on automated processing of personal data, including those intended to define the individual, consumption, and credit profile or aspects of the holder's personality.
[4] Available at: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=RESOLU%C3%87%C3%83O%20CMN&numero=4893>. Accessed on: March 16, 2023
[5] Available at:
[6] <https://www.bcb.gov.br/estabilidadefinananceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=85>. Accessed on: March 16, 2023.

2 BANK SECRECY

Complementary Law 105/2001 ("Banking Secrecy Law") regulates the confidentiality of information and bank data of individuals and companies, applying to transactions carried out in financial institutions, fintechs, and other companies in the financial market.

The mentioned law lists as non-violation of the duty of secrecy the following hypotheses:

the sharing of information between financial institutions for registration purposes

providing registration information to credit protection entities

sharing financial and payment data to database managers to form credit history, among other situations etc

In addition, the Banking Secrecy Law establishes in which specific situations bank secrecy may be breached, such as, for example, in the event of a court order or request from tax and regulatory authorities, and when necessary for investigations of money laundering, evasion tax, or other financial crimes.

3 FRAUD PREVENTION

With the expansion of the digital economy, criminals operating in the virtual world can exploit the technologies used by fintechs to carry out illicit practices, such as identity theft, money laundering, and financial fraud, among others . As such, fraud prevention is critical to the industry and must be addressed using appropriate technology. With the expansion of the digital economy, criminals operating in the virtual world can exploit the technologies

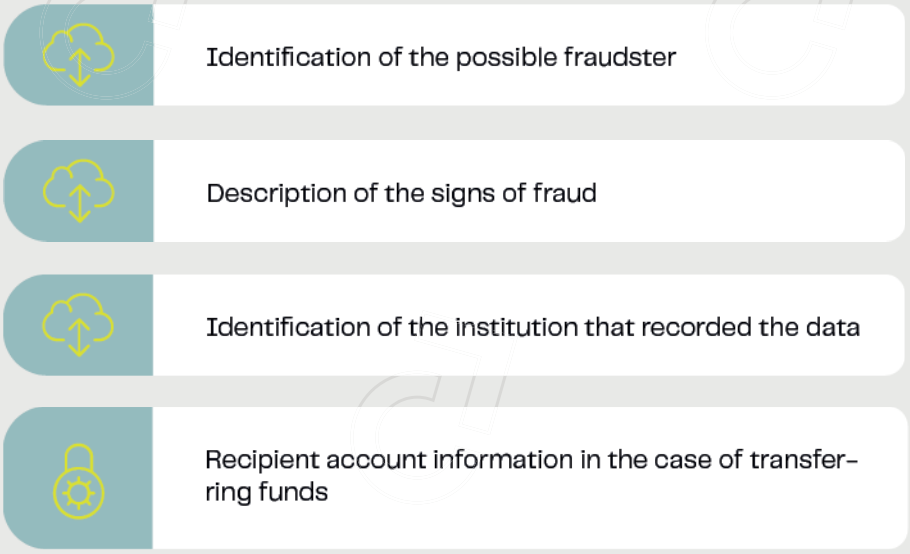
7 Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm>. Acesso em: 16 mar. 2023.

In this sense, BACEN published Joint Resolution No. 6 ("Resolution") of May 23, 2023[8], establishing requirements for sharing data and information on signs of fraud between financial institutions, payment institutions, and other authorized entities operated by the Central Bank.

The resolution addresses information asymmetry in the financial sector, recognizing that fraudsters often attempt to commit their acts in different financial institutions. Data sharing is a crucial tool to enable institutions to identify suspicious patterns and fraudulent activities more quickly and effectively.

One of the most controversial points of the resolution is the provision of the need for customer consent to carry out fraud prevention activities, creating many challenges in the joint interpretation of privacy and data protection laws, particularly the LGPD.

One of the main guidelines of the resolution is interoperability between electronic systems to be implemented by financial institutions, ensuring that all information is shared in a compatible manner. This sharing must include the following information:



The responsibility for data processing remains in the financial institutions, which shall comply with the standards established by legislation, such as the LGPD. It is necessary to obtain customers' prior and general consent to record data related to them, and this requirement must be highlighted in contracts or valid legal instruments.

These measures aim to create a safer environment for financial transactions, sharing the responsibility for combating fraud among all parties involved.

For fraud prevention, organizations must adopt compliance programs, implement robust compliance and customer assessment processes, risk analysis, continuous monitoring, implementation of cybersecurity policies, and incident response plans. In addition, it is important that organizations also adopt technological information security measures, such as multifactor authentication, data encryption, facial recognition technology, and artificial intelligence, among other resources. However, such resources must always be used following current legislation, mainly due to the possible risk of discrimination in certain technologies. For example, artificial intelligence algorithms can discriminate in some customer and user reviews.

[8] Available at: <Exibe Normativo (bcb.gov.br)>. It was accessed on 18 September 2023.

4

GOOD PAYORS' REGISTRY

Law No. 12,414/2011 ("Good Payors' Act") created a register[9] that gathers information on consumer delinquency and can be used as a basis for credit analysis to increase the supply of credit and reduce interest rates for consumers with a good payment history.

Fintechs that offer credit analysis services, loans, and other financial services with lower interest rates can use register information to assess their customers' credit risk.

However, to use the information from the Good Payors Act, fintechs must comply with the provisions of this law, which establishes rules for using this data.

Among the main provisions of this law, we highlight the need to inform data subjects about the inclusion of their information in the register, the possibility of contesting the information, and the prohibition of discrimination by companies.

In summary, the Good Payors Act is an important tool for risk analysis and credit granting in Brazil. Its applicability to fintech is relevant so that fintechs that use the information from the register must comply with the provisions of the mentioned law and the LGPD, protecting its customers' data and avoiding abusive practices in the credit market.

5

OPEN FINANCE

Open Finance is an evolution of the concept of Open Banking in that it expands its scope to encompass financial services, such as foreign exchange, investments, accreditation, insurance, and pensions. With the user's express authorization, institutions participating in Open Finance can access the user's history for analysis and offer personalized services.

Given this, information security is one of the main concerns of the institutions participating in this new system, so they must comply with the rules of the CMN and Bacen related to the sharing of information. Data sharing requires user consent, identity authentication, and confirmation, as well as implementation of standards[10] and operational procedures, cybersecurity rules, and encryption of shared data. Also, partnerships with institutions not authorized to operate by Bacen should be avoided.

Regarding the Open Finance data and information sharing structure, the so-called APIs (Application Programming Interfaces) will be the bridge between the institutions participating in Open Finance, allowing the sharing of customer data. APIs are "key enablers of new business and innovation"[11] in Open Finance. Still, it's important to remember that the technology comes with risks, such as serious privacy breaches, intrusions, and attacks on systems. Therefore, the security and privacy of customer data must be a priority for Open Finance participants, who must increasingly invest in cybersecurity.

9 Available at: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. It was accessed on 16 March 2023.

10 BACEN. Open Finance. Available at: <https://www.bcb.gov.br/estabilidadefinanceira/openfinance>. It was accessed on March 16, 2023.

11 SENSIDIA, PWC. Report on Digital Strategies with APIs in Latin America (online). Available at: <https://content.sensedia.com/hubfs/Report_o_estado_das%20APIs_ nal_v2.pdf>. Accessed on: March 16, 2023

Our recognitions

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 & 2022)

Leaders League (2021, 2022 & 2023)

Transactional Track Record (2021 & 2022)

The Legal 500 (2022)

Meet our Partners

Alan Campos Thomaz

Partner

Technology & Digital Business, Privacy and Data Protection, Fintechs and Intellectual Property

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Sérgio Meirelles

Partner

Corporate, M&A, Venture Capital and Wealth

sergio@camposthomaz.com

+55 11 9 7551.9865

Filipe Starzynski

Partner

Litigation & Law Enforcement, Civil, Real State, Labor and Family

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Partner

Intellectual Property, Technology, Agreement and Regulatory

juliana@camposthomaz.com

+55 11 9 8644.1613

Follow us

campos thomaz & meirelles advogados

Subscribe to our newsletter