Cloud Compliance Center - Brazil

| Contents |
| --- |
| To generate table of contents, right-click here and select **Update Field.** |

BRAZIL

*This content was last reviewed around March 2023.*

**Cloud-friendly**

**1. Are financial institutions legally permitted to use cloud services?**

Yes, there is no prohibition on using cloud services under applicable regulatory laws.

**2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?**

Yes, there are several measures. First, Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), provides for cybersecurity policy and requirements for data processing and storage and cloud computing services to be followed by financial institutions and similar entities. In this context, Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**"), regulates these matters with respect to payment institutions.

Additionally, Brazilian Securities and Exchange Commission ("**SEC**") Resolution No. 35, effective as of 26 May 2021 ("**Resolution 35**"), establishes rules and proceedings to be followed in respect of the intermediation of securities on regulated securities markets by the entities under its supervision (for example, brokers).

Cloud services, including processing and storage of data provided offshore, must also observe, among other issues, the following, pursuant to Article 16 of Resolution 4,893 and Resolution 85:

An agreement to exchange information between the BCB and the regulatory authorities of the countries where the services are provided.

A contracting financial or payment institution must ensure that the provision of services does not damage its regular functioning nor hinder BCB activities.

A contracting financial or payment institution must define, prior to retaining services, the countries and regions (in each country) where those services may be provided and where data may be stored, processed and managed.

A contracting financial or payment institution must establish alternatives for the continuity of its business activities, in case the cloud service agreement is terminated or becomes impossible to maintain.

**3. Are there any specific contractual requirements for cloud outsourcing?**

Yes. According to Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), and Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**"), the contract must refer, among other issues, to the following:

Audit rights: Pursuant to Article 21 of Resolution 4,893 and Resolution 85, a financial or payment institution must have in place monitoring and control mechanisms to ensure the implementation and effectiveness of their cybersecurity policy, the action and response plan for incidents, and the requirements for contracting data processing and storage and cloud computing services. Such mechanisms should be subject to periodic testing by the payment or financial institution's internal audit.

The use of subcontractors: Pursuant to Article 17 of Resolution 4,893 and Resolution 85, subcontractors are allowed provided that the cloud service provider agreement stipulates that the cloud service provider is obliged to notify the contractor of any subcontractors.

Technical and organizational measures or ICT guidelines, including security requirements: Pursuant to Article 2 of Resolution 4,893 and Resolution 85, a financial and payment institution must adopt, implement and keep cybersecurity policies based on principles and directives regarding confidentiality, integrity and data availability. Such policies must be compatible with the size, business model and risk profile of the financial or payment institution, the nature and complexity of transactions and products, as well as data sensitivity.

Business continuity/disaster recovery: Pursuant to Article 12, II, of Resolution 4,893 and Resolution 85, a financial or payment institution must verify the cloud service provider's capacity to support data recovery. Such verification must be documented.

Pursuant to Article 17 of Resolution 4,893 and Resolution 85, the cloud service agreement must contain, among other provisions, these terms and conditions:

An indication of the countries and regions in each country where the services may be provided and data may be stored, processed and managed

Adoption of security measures for the transmission and storage of data

Maintenance, while the contract is in force, of data segregation and access controls to protect end users' information

If the agreement is terminated, an obligation to transfer the data to the new cloud service provider or to the contracting financial or payment institution, and an obligation for the replaced contractor to remove the data after it has been transferred to the new cloud service provider and its integrity and availability is confirmed

A contracting financial or payment institution's access to (i) information provided by the outsourcing company, (ii) information regarding the service provider's certifications and specialized audit reports and (iii) information and resource management suitable for monitoring the services to be provided

A service provider's obligation to notify the financial or payment institution on the subcontracting of relevant services to the financial or payment institution

The BCB's permission to access contracts and agreements signed for the provision of the services, documentation and information related to the services provided, stored data and information about their processing, copies of security of data and information, as well as access codes to data and information

The adoption of measures by the financial or payment institution, due to any specific determination by the BCB

A service provider's obligation to keep the financial or payment institution permanently informed of any limitations that may affect the provision of services or compliance with current legislation and regulations

In the case of resolution, the cloud service provider's obligation to grant full access to the entity responsible for the resolution of all data content stored by the cloud service provider

Thirty days' prior notice by the cloud service provider for the termination of the services in the case of default or resolution of the contracting financial or payment institution

From a Brazilian General Data Protection Law (Law 13,709/2018 — "**LGPD**") perspective, it is recommended that processing instructions and international data transfers are addressed in a data processing agreement ("**DPA**") with the cloud service provider.

Please note that, although the LGPD does not expressly require the parties to enter into a DPA, representatives from the Brazilian Data Protection Authority ("**ANPD**") have stated publicly that it consider this to be best practice. Therefore, it is highly recommended that a DPA is implemented in the context of cloud outsourcing.

**4. When does cloud outsourcing fall within the scope of the rules?**

Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), and Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**"), will apply to cloud outsourcing.

According to Resolution 4,893 and Resolution 85, cloud outsourcing services include the availability (on demand and virtually) to the contracting financial or payment institution of at least one of the following services: (i) data processing, data storage, network infrastructure and other computing resources that enable the contracting party to deploy or execute software, which may include operating systems and applications developed by the contracting party or acquired by it; (ii) deployment or execution of applications developed by the contracting party, or acquired by it, using the cloud service provider's computing resources; or (iii) implementation via the internet of applications implemented or developed by the cloud service provider, using the cloud service provider's own computing resources. Please refer to Q&A No. 7 on when the Brazilian General Data Protection Law (Law 13,709/2018 — "**LGPD**") will apply in cases of cloud outsourcing.

**5. Does the outsourcing need to be notified to the regulator?**

The Brazilian Central Bank ("**BCB**") must be notified within 10 days of hiring the cloud service provider. Such notification must contain the following:

Name of the cloud service provider

Relevant services provided

Indication of the countries and regions of each country where services are to be provided and data may be stored, processed or managed

The BCB's prior approval must be obtained if the financial institution or payment institution retains a cloud service provider in countries where there is no agreement to exchange information between the BCB and the competent authorities. The financial institution or payment institution must request such approval from the BCB at least 60 days before retaining the cloud services in question.

**6. What are the potential consequences for breaching financial services rules on cloud outsourcing?**

The Brazilian Central Bank may restrict or terminate any outsourcing cloud services relationship for breaching rules, including terminating the data cloud agreement with the financial or payment institution.

Civil, criminal and administrative penalties could be imposed if the breach causes damage to the users and/or to the financial system and/or if the breach were classified as an administrative or criminal offense.

**7. Are there any data privacy and/or data security laws that would apply?**

Yes, the Brazilian General Data Protection Law (Law 13,709/2018 — "**LGPD**") will apply to cloud services to the extent that the cloud services provider performs the following:

(i) Processes personal data (or personal data collected) in Brazil

(ii) Processes personal data for the provision of goods or services, or when the processing activities have as their purpose the processing of data of individuals located in Brazil

For the purposes of the LGPD, personal data is deemed as "any information related to an individual identified or identifiable." Processing is deemed as "any operation carried out with personal data, as those that refer to collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, storing, archiving, elimination, evaluation, control, modification, communication, transfer or extraction."

The LGPD is the first comprehensive data protection law in Brazil and was "inspired" by the European data protection law ("**GDPR**"). The principles and general obligations are similar to the GDPR, but not identical. Some of the key obligations imposed on companies that process personal data under the LGPD are as follows:

To map all processing activities and maintain a record of processing activities

To process personal data only according to the legal basis for processing as set forth under the law

To comply with data subjects' rights

To notify the authority and data subjects in certain cases of security incidents

To appoint a data protection officer

To adopt technical, organizational and security measures

To take additional steps in the case of international data transfers

To provide transparency to personal data subjects about the data processing activities, by making available a privacy notice with clear, accurate and easily accessible information

To comply with the principles set forth in the LGPD

The list above is not exhaustive and may need to be adjusted depending on the case. These obligations may also vary depending on whether the company acts as a data processor or controller.

Additionally, Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), and Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**"), provide that financial and payment institutions located in Brazil, when hiring cloud service providers, must implement a policy for cybersecurity and follow the requirements for contracting data processing and storage and cloud computing services.

Please refer to Q&A No. 2 for provisions regarding offshore data processing by cloud services set forth in Resolution 4,893 and Resolution 85.

**8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?**

Yes. According to the Brazilian General Data Protection Law (Law 13,709/2018 — "**LGPD**"), international transfers are only permitted in specific circumstances, including the following:

When the foreign country or international organization provides an adequate level of data protection, as assessed by the Brazilian Data Protection Authority (“**BDPA**”).

When the transfer is authorized by the BDPA

When the data controller can show and guarantee that the conditions established by the LGPD are met, which can be accomplished through specific contractual clauses for the said transfer, standard contractual clauses (SCCs), binding corporate rules or third-party certification — all of which must be approved by the BDPA

When the data subject has consented specifically and clearly to the international transfer, having been informed previously about the international nature of the transfer (The transfer of data must be separate from other purposes of processing personal data.)

To comply with a legal obligation to which the original controller is subject

This is one of the areas of the LGPD that relies extensively on the regulations of the BDPA. However, the authority has not issued any guidance or regulations on this point yet.

As the LGPD is similar to the GDPR and follows the same principles, EU SCCs are likely to be acceptable, subject to minor amendments such as wording, definitions and references to the LGPD's equivalent legal provisions, instead of the GDPR's.

Additionally, there are obligations set forth in Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), and Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**").

Please refer to Q&A No. 2 for provisions regarding cloud services processing of data offshore contained in Resolution 4,893 and Resolution 85.

**9. Does a cloud service provider need a financial services authorization or license to provide cloud services?**

No, a license is not required.

**10. Is express consent from customers or other data subjects required before moving data to the cloud?**

Not necessarily. From a data protection perspective, the Brazilian General Data Protection Law ("**LGPD**") requires a legal basis for each processing activity. The data subject's consent is just one of the 10 available legal bases for data processing. Therefore, this should be assessed on a case-by-case basis, depending on the legal basis relevant for processing.

If no personal data is included, the LGPD provisions are not applicable.

From a banking perspective, since a cloud service provider will not have access to financial data, which will be encrypted in the cloud and the cloud service provider will not hold the encryption key, consent will not be required.

**11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?**

There are no specific local laws that require a cloud service provider to be able to access the data it hosts.

Nonetheless, please note that Law 12,965/2014 provides that the cloud service provider may be required to disclose any client records, data or communications pursuant only to a valid court order.

**12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?**

Yes. Cloud service providers may be required to disclose any client data pursuant to a valid court order in Brazil, in accordance with Law 12,965/2014 ("**Brazilian Internet Legal Framework**"). Furthermore, Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), and Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**"), require a contractual provision between cloud service providers and financial and payment institutions permitting the BCB to access data stored and information.

# Permissibility of cloud

## 1. Are financial institutions legally permitted to use cloud services?

Yes, there is no prohibition on using cloud services under applicable regulatory laws.

# Rules for cloud outsourcing

## 2. Are there any rules that apply to cloud use by financial institutions (e.g., rules regarding outsourcing or the use of cloud services)?

Yes, there are several measures. First, Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), provides for cybersecurity policy and requirements for data processing and storage and cloud computing services to be followed by financial institutions and similar entities. In this context, Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**"), regulates these matters with respect to payment institutions.

Additionally, Brazilian Securities and Exchange Commission ("**SEC**") Resolution No. 35, effective as of 26 May 2021 ("**Resolution 35**"), establishes rules and proceedings to be followed in respect of the intermediation of securities on regulated securities markets by the entities under its supervision (for example, brokers).

Cloud services, including processing and storage of data provided offshore, must also observe, among other issues, the following, pursuant to Article 16 of Resolution 4,893 and Resolution 85:

An agreement to exchange information between the BCB and the regulatory authorities of the countries where the services are provided.

A contracting financial or payment institution must ensure that the provision of services does not damage its regular functioning nor hinder BCB activities.

A contracting financial or payment institution must define, prior to retaining services, the countries and regions (in each country) where those services may be provided and where data may be stored, processed and managed.

A contracting financial or payment institution must establish alternatives for the continuity of its business activities, in case the cloud service agreement is terminated or becomes impossible to maintain.

# Contract requirements

## 3. Are there any specific contractual requirements for cloud outsourcing?

Yes. According to Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), and Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**"), the contract must refer, among other issues, to the following:

Audit rights: Pursuant to Article 21 of Resolution 4,893 and Resolution 85, a financial or payment institution must have in place monitoring and control mechanisms to ensure the implementation and effectiveness of their cybersecurity policy, the action and response plan for incidents, and the requirements for contracting data processing and storage and cloud computing services. Such mechanisms should be subject to periodic testing by the payment or financial institution's internal audit.

The use of subcontractors: Pursuant to Article 17 of Resolution 4,893 and Resolution 85, subcontractors are allowed provided that the cloud service provider agreement stipulates that the cloud service provider is obliged to notify the contractor of any subcontractors.

Technical and organizational measures or ICT guidelines, including security requirements: Pursuant to Article 2 of Resolution 4,893 and Resolution 85, a financial and payment institution must adopt, implement and keep cybersecurity policies based on principles and directives regarding confidentiality, integrity and data availability. Such policies must be compatible with the size, business model and risk profile of the financial or payment institution, the nature and complexity of transactions and products, as well as data sensitivity.

Business continuity/disaster recovery: Pursuant to Article 12, II, of Resolution 4,893 and Resolution 85, a financial or payment institution must verify the cloud service provider's capacity to support data recovery. Such verification must be documented.

Pursuant to Article 17 of Resolution 4,893 and Resolution 85, the cloud service agreement must contain, among other provisions, these terms and conditions:

An indication of the countries and regions in each country where the services may be provided and data may be stored, processed and managed

Adoption of security measures for the transmission and storage of data

Maintenance, while the contract is in force, of data segregation and access controls to protect end users' information

If the agreement is terminated, an obligation to transfer the data to the new cloud service provider or to the contracting financial or payment institution, and an obligation for the replaced contractor to remove the data after it has been transferred to the new cloud service provider and its integrity and availability is confirmed

A contracting financial or payment institution's access to (i) information provided by the outsourcing company, (ii) information regarding the service provider's certifications and specialized audit reports and (iii) information and resource management suitable for monitoring the services to be provided

A service provider's obligation to notify the financial or payment institution on the subcontracting of relevant services to the financial or payment institution

The BCB's permission to access contracts and agreements signed for the provision of the services, documentation and information related to the services provided, stored data and information about their processing, copies of security of data and information, as well as access codes to data and information

The adoption of measures by the financial or payment institution, due to any specific determination by the BCB

A service provider's obligation to keep the financial or payment institution permanently informed of any limitations that may affect the provision of services or compliance with current legislation and regulations

In the case of resolution, the cloud service provider's obligation to grant full access to the entity responsible for the resolution of all data content stored by the cloud service provider

Thirty days' prior notice by the cloud service provider for the termination of the services in the case of default or resolution of the contracting financial or payment institution

From a Brazilian General Data Protection Law (Law 13,709/2018 — "**LGPD**") perspective, it is recommended that processing instructions and international data transfers are addressed in a data processing agreement ("**DPA**") with the cloud service provider.

Please note that, although the LGPD does not expressly require the parties to enter into a DPA, representatives from the Brazilian Data Protection Authority ("**ANPD**") have stated publicly that it consider this to be best practice. Therefore, it is highly recommended that a DPA is implemented in the context of cloud outsourcing.

# Regulated cloud outsourcing

## 4. When does cloud outsourcing fall within the scope of the rules?

Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), and Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**"), will apply to cloud outsourcing.

According to Resolution 4,893 and Resolution 85, cloud outsourcing services include the availability (on demand and virtually) to the contracting financial or payment institution of at least one of the following services: (i) data processing, data storage, network infrastructure and other computing resources that enable the contracting party to deploy or execute software, which may include operating systems and applications developed by the contracting party or acquired by it; (ii) deployment or execution of applications developed by the contracting party, or acquired by it, using the cloud service provider's computing resources; or (iii) implementation via the internet of applications implemented or developed by the cloud service provider, using the cloud service provider's own computing resources. Please refer to Q&A No. 7 on when the Brazilian General Data Protection Law (Law 13,709/2018 — "**LGPD**") will apply in cases of cloud outsourcing.

# Regulatory notifications

## 5. Does the outsourcing need to be notified to the regulator?

The Brazilian Central Bank ("**BCB**") must be notified within 10 days of hiring the cloud service provider. Such notification must contain the following:

Name of the cloud service provider

Relevant services provided

Indication of the countries and regions of each country where services are to be provided and data may be stored, processed or managed

The BCB's prior approval must be obtained if the financial institution or payment institution retains a cloud service provider in countries where there is no agreement to exchange information between the BCB and the competent authorities. The financial institution or payment institution must request such approval from the BCB at least 60 days before retaining the cloud services in question.

# Consequences of regulatory breach

## 6. What are the potential consequences for breaching financial services rules on cloud outsourcing?

The Brazilian Central Bank may restrict or terminate any outsourcing cloud services relationship for breaching rules, including terminating the data cloud agreement with the financial or payment institution.

Civil, criminal and administrative penalties could be imposed if the breach causes damage to the users and/or to the financial system and/or if the breach were classified as an administrative or criminal offense.

# Data privacy and security

## 7. Are there any data privacy and/or data security laws that would apply?

Yes, the Brazilian General Data Protection Law (Law 13,709/2018 — "**LGPD**") will apply to cloud services to the extent that the cloud services provider performs the following:

(i) Processes personal data (or personal data collected) in Brazil

(ii) Processes personal data for the provision of goods or services, or when the processing activities have as their purpose the processing of data of individuals located in Brazil

For the purposes of the LGPD, personal data is deemed as "any information related to an individual identified or identifiable." Processing is deemed as "any operation carried out with personal data, as those that refer to collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, storing, archiving, elimination, evaluation, control, modification, communication, transfer or extraction."

The LGPD is the first comprehensive data protection law in Brazil and was "inspired" by the European data protection law ("**GDPR**"). The principles and general obligations are similar to the GDPR, but not identical. Some of the key obligations imposed on companies that process personal data under the LGPD are as follows:

To map all processing activities and maintain a record of processing activities

To process personal data only according to the legal basis for processing as set forth under the law

To comply with data subjects' rights

To notify the authority and data subjects in certain cases of security incidents

To appoint a data protection officer

To adopt technical, organizational and security measures

To take additional steps in the case of international data transfers

To provide transparency to personal data subjects about the data processing activities, by making available a privacy notice with clear, accurate and easily accessible information

To comply with the principles set forth in the LGPD

The list above is not exhaustive and may need to be adjusted depending on the case. These obligations may also vary depending on whether the company acts as a data processor or controller.

Additionally, Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), and Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**"), provide that financial and payment institutions located in Brazil, when hiring cloud service providers, must implement a policy for cybersecurity and follow the requirements for contracting data processing and storage and cloud computing services.

Please refer to Q&A No. 2 for provisions regarding offshore data processing by cloud services set forth in Resolution 4,893 and Resolution 85.

# Overseas hosting

## 8. Are there any restrictions under local data protection laws that would impact the overseas hosting of data?

Yes. According to the Brazilian General Data Protection Law (Law 13,709/2018 — "**LGPD**"), international transfers are only permitted in specific circumstances, including the following:

When the foreign country or international organization provides an adequate level of data protection, as assessed by the Brazilian Data Protection Authority (“**BDPA**”).

When the transfer is authorized by the BDPA

When the data controller can show and guarantee that the conditions established by the LGPD are met, which can be accomplished through specific contractual clauses for the said transfer, standard contractual clauses (SCCs), binding corporate rules or third-party certification — all of which must be approved by the BDPA

When the data subject has consented specifically and clearly to the international transfer, having been informed previously about the international nature of the transfer (The transfer of data must be separate from other purposes of processing personal data.)

To comply with a legal obligation to which the original controller is subject

This is one of the areas of the LGPD that relies extensively on the regulations of the BDPA. However, the authority has not issued any guidance or regulations on this point yet.

As the LGPD is similar to the GDPR and follows the same principles, EU SCCs are likely to be acceptable, subject to minor amendments such as wording, definitions and references to the LGPD's equivalent legal provisions, instead of the GDPR's.

Additionally, there are obligations set forth in Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), and Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**").

Please refer to Q&A No. 2 for provisions regarding cloud services processing of data offshore contained in Resolution 4,893 and Resolution 85.

# Financial services authorizations licenses

## 9. Does a cloud service provider need a financial services authorization or license to provide cloud services?

No, a license is not required.

# Customer data subject consent

## 10. Is express consent from customers or other data subjects required before moving data to the cloud?

Not necessarily. From a data protection perspective, the Brazilian General Data Protection Law ("**LGPD**") requires a legal basis for each processing activity. The data subject's consent is just one of the 10 available legal bases for data processing. Therefore, this should be assessed on a case-by-case basis, depending on the legal basis relevant for processing.

If no personal data is included, the LGPD provisions are not applicable.

From a banking perspective, since a cloud service provider will not have access to financial data, which will be encrypted in the cloud and the cloud service provider will not hold the encryption key, consent will not be required.

# Data access requirements

## 11. Are there any local laws that require a cloud service provider to be able to access the data it hosts?

There are no specific local laws that require a cloud service provider to be able to access the data it hosts.

Nonetheless, please note that Law 12,965/2014 provides that the cloud service provider may be required to disclose any client records, data or communications pursuant only to a valid court order.

# Data disclosure requirements

## 12. Are there any local laws that would require a cloud service provider to disclose the data it hosts to any third parties in any circumstances (including regulatory or law enforcement authorities)?

Yes. Cloud service providers may be required to disclose any client data pursuant to a valid court order in Brazil, in accordance with Law 12,965/2014 ("**Brazilian Internet Legal Framework**"). Furthermore, Brazilian National Monetary Council ("**CMN**") Resolution No. 4,893, effective as of 26 February 2021 ("**Resolution 4,893**"), and Brazilian Central Bank ("**BCB**") Resolution No. 85, effective as of 8 April 2021 ("**Resolution 85**"), require a contractual provision between cloud service providers and financial and payment institutions permitting the BCB to access data stored and information.

©Copyright © 2025 Baker & McKenzie. All rights reserved. **Ownership**: This documentation and content (Content) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms). The Content is protected under international copyright conventions. Use of this Content does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion**: All Content is for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulations and practice are subject to change. The Content is not offered as legal or professional advice for any specific matter. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any Content. Baker McKenzie and the editors and the contributing authors do not guarantee the accuracy of the Content and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the Content. The Content may contain links to external websites and external websites may link to the Content. Baker McKenzie is not responsible for the content or operation of any such external sites and disclaims all liability, howsoever occurring, in respect of the content or operation of any such external websites. **Attorney Advertising**: This Content may qualify as “Attorney Advertising” requiring notice in some jurisdictions. To the extent that this Content may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. **Reproduction**: Reproduction or copying of the Content on this Site without express written authorization is strictly prohibited.