Cloud Compliance Center - Brazil

Contract requirements

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

# 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.

©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.