Cloud Compliance Center - Mexico

Data privacy and security

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

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

Yes. General data privacy regulations — primarily, the Federal Law for the Protection of Personal Data Held by Private Entities ("Ley Federal de Proteccion de Datos personales en Posesión de los Particulares") (LFPDPPP) — regulates how financial institutions handle the personal data of data subjects, such as employees, customers, users, suppliers, contractors and even cloud service providers.

Under the LFPDPPP, data controllers are restricted from contracting with cloud service providers that do not ensure proper protection of personal data, and they must not include terms or conditions in their contracts that would authorize or permit a cloud service provider to assume the ownership of personal data.

The LFPDPPP also requires a data controller to put in place a data processor agreement with an unrelated third party that will manage hosted personal data for the data controller. The data processor agreement must include certain terms, including provisions setting out the data processor's obligations and liabilities, restrictions relating to the data, and security measures to be taken.

Additionally, the Ministry of Economy and the data privacy authorities have issued a joint publication of the Minimum Suggested Criteria that Should be Considered for Contracting Cloud Computing Services that Involve Processing of Personal Data ("Criterios mínimos sugeridos para la contratación de servicios de cómputo en la nube que impliquen el tratamiento de Datos Personales," "**MSC Document**"). Given the collaborative nature of this document, not all the recommendations are specifically privacy-related. However, the MSC Document offers insight on the rationale and scope of the regulatory requirements. From the MSC Document, it can be inferred that a cloud service would be considered "secure" when data controllers do the following:

(a) Carry out certain pre-contractual screening of the cloud providers

(b) Ensure they are able to maintain control over their information placed in the cloud through contractual and technical mechanisms

(c) Ensure security measures are in place to protect the information

The MSC Document confirms that data controllers are liable for selecting and contracting the right cloud providers and that failure to carry out the minimum required tests appropriately would result in a breach of the Accountability Principle in the LFPDPPP and may be subject to fines.

Conversely, the MSC Document clarifies that cloud service providers are not legally mandated to include literally the requirements of Section 52 of the LFPDPPP in their contractual terms to convince customers that their services are compliant. Conversely, customers may use product literature, technical controls and other information that cloud service providers may offer to clients to evaluate the service as a whole and conclude whether their cloud offering is "secure." It is also clarified that cloud providers are subject to the general regime applicable to data processors, including, for instance, provisions related to subcontracting.

It is recommended to encrypt data hosted in a cloud service to protect the confidentiality of users' data. However, this is not a mandatory requirement under the applicable laws or regulations.

©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.