Complying with Mexico's Data Privacy Rules: 6 Key Tips for U.S. and Other Foreign Businesses

Insights
8.15.24

Una versión en español de esta Insight está disponible haciendo clic arriba.

Companies doing business in Mexico should review relevant policies and practices to ensure they align with the country's comprehensive data privacy framework. Specifically, you'll want to assess your privacy notices, data processing policies, and security measures aimed at protecting personal data. By taking effective measures now you can help ensure legal compliance, foster trust among stakeholders, mitigate risks associated with data breaches, and avoid sanctions. Here are six key tips for U.S. and other foreign businesses as you navigate the data privacy laws in Mexico that impact your operations – including an action plan to boost your compliance strategy.

1. Understand the Regulatory Environment

The Federal Institute for Access to Information and Data Protection (INAI) plays a pivotal role, serving as the main regulatory body for protecting personal data, overseeing compliance, and issuing guidelines related to privacy rules. The INAI has the following powers:

- **Oversight and Surveillance:** Ensuring compliance with legislation on personal data protection and monitoring enforcement, while also establishing specific criteria, recommendations, and guidelines.
- **Information and Education:** Providing information to individuals about their personal data rights and submitting an annual report to the Congress of the Union.
- **Verification and Sanctions:** Initiating verification procedures either on its own or upon request and exercising sanctioning powers.

You should also note the state-level Local Institutes for Access to Information and Data Protection, which are similar to the INAI but focus on state-specific issues regarding transparency and accountability.

2. Review the Key Data Privacy Laws

Mexico's data protection standards are aligned with international practices that promote transparency and accountability for organizations that handle personal information. Key legislation

and agreements include:

The Mexican Privacy Law (formally called the Federal Law for the Protection of Personal Data Held by Private Parties) is the primary legislation protecting personal data held by private parties. There is also the General Law for the Protection of Personal Data in the Possession of Obliged Subjects, which applies to data held by public-sector entities, including government agencies.

Notably, under Mexican law, data owners have the following ***four rights (known as ARCO Rights):***

- **Access**: Right to access their data, as well as the applicable privacy notice.
- **Rectification**: Right to correct their data when it is inaccurate or incomplete.
- **Cancellation**: Right to delete their personal data following a period of blocking.
- **Opposition:** Right to oppose, at any time and for legitimate reasons, the processing of their personal data.

State-Specific Data Protection Laws: Each state may have additional regulations enforced by local institutes.

United States-Mexico-Canada Agreement (USMCA/T-MEC) – In addition to federal, state, and local rules, several international treaties impact data privacy, including the USMCA (which is known as T-MEC in Mexico).

Key regulations include the following:

- Regulations to the Federal Law on Protection of Personal Data Held by Private Parties
- Privacy Notice Rules
- Binding Self-Regulation Parameters
- General Guidelines for the Protection of Personal Data for the public sector (federal, state, or local authorities)

3. Comply with General Data Transfer Rules

The Mexican Privacy Law impacts **data controllers** who make decisions about processing personal data and **data processors** who handle personal data on behalf of the data controller. Compliance with general data transfer rules includes:

- **Transfer Conditions:** Data controllers may freely transfer personal data to domestic or foreign third parties if the privacy notice allows and the data owner has not opted out.
- **Purpose Limitation:** Personal data can only be transferred for purposes authorized by the data owner's opt-out or opt-in consent as stated in the privacy notice.

- **Third-Party Obligations:** The recipient of the personal data assumes the same obligations as the data controller that transferred the data.
- **International Agreements:** Rules for data transfer under international treaties are also important to understand, for example, the USMCA generally prohibits requirements for data localization, meaning member countries cannot mandate that data must be stored or processed exclusively within their borders as a condition for conducting business.

Notably, Mexico's data protection law is not limited to data controllers established or operating in Mexican territories. Rather, under the applicable regulations, the rules also apply to companies that are subject to Mexican legislation under the terms of a contract or international law — and noncompliance can result in steep penalties.

4. Note Exemptions to Data Transfer Rules

Domestic or international transfers of personal data may be carried out without the explicit consent of the data owner in specific cases, including:

- **Legal or Treaty Requirements:** The transfer is necessary pursuant to a law or treaty to which Mexico is a party.
- **Medical Necessity:** The transfer is essential for medical diagnosis, prevention, healthcare delivery, medical treatment, or health services management.
- **Corporate Affiliates:** The transfer is made to holding companies, subsidiaries, or affiliates under common control with the data controller, or to a parent company or any company within the same group, operating under the same internal processes and policies.
- **Contractual Necessity:** The transfer is required by virtue of a contract executed or to be executed between the data controller and a third party in the interest of the data owner.

5. Create Your Action Plan

Under the Mexican Privacy Law, companies should have certain elements and documents in place, such as:

- **Privacy Notice:** Inform individuals on how their personal data will be handled, including purposes, use, and rights. Ensure the notice complies with applicable guidelines.
- **Data Processing Policies and Procedures:** Develop internal policies that outline how personal data is collected, used, stored, and protected.
- **Data Protection Measures:** Implement security measures to safeguard personal data against unauthorized access, loss, or damage.
- **Consent Mechanisms:** Develop procedures to obtain consent from individuals before collecting or processing their personal data.

- **Access and Rights Management:** Create processes for data owners to exercise their ARCO Rights mentioned above (access, rectification, cancellation, and opposition).
- **Data Breach Response Plan:** Implement protocols to detect, respond to, and mitigate the impact of data breaches.
- **Data Transfer Agreements:** Ensure your contracts or agreements with third parties that receive personal data cover compliance with data protection principles.

You may also want to implement the following best practices that go beyond legal compliance:

- **Data Inventory:** Create a comprehensive list of the types of personal data collected, processed, and stored by the company.
- **Privacy Impact Assessments (PIAs):** Conduct assessments to evaluate the potential risks and impacts of data processing activities on individuals' privacy.
- **Records of Consent:** Maintain documentation proving that individuals have given their consent to process their personal data.
- **Training and Awareness Programs:** Educate employees on data protection principles and compliance requirements.
- **Annual Compliance Review:** Ensure ongoing compliance with privacy laws and regulations and make updates to policies and procedures as needed.

6. Track Potential Changes on the Horizon

Proposed reforms to Mexico's Constitution, including potential changes to the INAI's role, could significantly impact data protection regulations and transparency efforts in the future. Although these proposals have not been finalized, they include plans to eliminate independent bodies like the INAI, which could impact administrative burdens, costs, and transparency policies.

The Mexican Congress will debate these constitutional reforms once the new session begins in September 2024. So stay tuned for updates.

Conclusion

Keeping up with evolving privacy laws is crucial for companies doing business in Mexico. For more information on how this impacts your operations in Mexico, reach out to your Fisher Phillips attorney or the author of this Insight. Fisher Phillips Mexico is at your service to assist you with any questions related to this topic, as well as with any matter in labor law. Make sure you are subscribed to Fisher Phillips' Insight System to have the most up-to-date information sent directly to your inbox.

Related People

Héctor Cuevas
Partner
+55 5207 7300
Email

Service Focus

International

Privacy and Cyber

Counseling and Advice

Related Offices

Mexico