Last Updated: September 2025

FAQs re: Mexico's Federal Law for the Protection of Personal Data held by Private Parties of 2025

What are the privacy laws in Mexico?

Mexico's new Federal Law for the Protection of Personal Data held by Private Parties of 2025 ("LFPDPPP") came into force on March 21, 2025, introducing expanded obligations and protections for personal data processing. It revises the previous regime, strengthening oversight, enforcement mechanisms, and individual rights over personal data. Regulations under the previous law remain active until new implementation rules are released.

Do these laws apply to organizations outside of Mexico?

The LFPDPPP applies to all "persons" processing personal data in Mexico, with very limited exceptions. It applies regardless of where the organization is established if it processes data in Mexico, substantially broadening the law's reach.

What is "personal information" under LFPDDD?

Under the LFPDPPP, "personal data" refers to any information that can identify an individual, either directly or indirectly. The law includes sensitive, financial, and patrimonial data under strict regulation and protection.[1]

Is consent needed to collect personal information?

The LFPDPPP generally requires consent for the processing of personal information. Consent may be express or implied, except when processing sensitive, financial, or patrimonial data, or where another law requires express consent. The law also broadens exemptions, allowing consent to be waived by law, regulations, or administrative provisions. Individuals retain the right to withdraw consent and opt out of most processing activities.[2]

Is there a requirement to have a local representative or physical presence like a Privacy Office?

While the LFPDPPP does not explicitly require a Data Protection Officer (DPO) or a local privacy office, it does mandate organizations establish controls or mechanisms to ensure confidentiality in data processing. Entities must designate specific roles or systems to ensure compliance, mirroring DPO requirements found in other jurisdictions.[3]

---

[1] LFPDPPP, Chapter I, Article 2, V.
[2] LFPDPPP, Chapter II, Article 7.
[3] LFPDPPP, Chapter IV, Article 29

Is there a requirement to notify individuals or regulators in the event of a data breach?

Yes. The law requires organizations to notify affected individuals without undue delay if a data breach poses significant risks to their rights. Notifications must include details on the nature of the breach, the data involved, possible consequences, and the mitigation measures taken. The LFPDPPP also anticipates mandatory breach notifications to regulators, with the protocols to be set out in future regulations.[4]

Are contracts with third-party service providers required?

When transferring personal data to third parties—including service providers—data controllers must ensure that contracts impose confidentiality and security obligations equivalent to those in the LFPDPPP. This ensures consistent protection throughout all stages of data transfer and processing.[5]

Can we transfer personal data outside of Mexico?

Transfers of personal data beyond Mexico's borders are subject to strict requirements.[6] Controllers must guarantee that recipients comply with the same standards of confidentiality and security. Cross-border transfers are generally allowed if the destination country maintains adequate protection or the data subject expressly consents. Exceptions exist for contractual necessity, public interest, or legal allowances. Controllers remain accountable for data protection throughout transfers.

Do individuals have access and correction rights?

Individuals are granted ARCO rights—Access, Rectification, Cancellation, and Opposition. They can inquire about, correct, or request deletion of their personal data, and object to certain processing activities. Organizations must respond to these requests within a 20-day period, with a possible 15-day extension for resolution. The law also safeguards individuals against automated decision-making, such as AI, ensuring human agency.[7]

What are the penalties for non-compliance?

The law is enforced by the Ministry of Anti-Corruption and Good Governance, empowered to investigate violations, issue warnings, and impose fines between 100 and 320,000 times the Unit of Measurement and Update (UMA).[8] Penalties double if sensitive personal data is involved. Severe breaches, especially those for profit or involving sensitive data, may result in imprisonment of up to five years, or double for egregious violations.

---

[4] LFPDPPP, Chapter II, Article 19.
[5] LFPDPPP Regulations, Chapter II, Article 51.
[6] 4 LFPDPPP, Chapter V, Article 35.
[7] LFPDPPP, Chapter III, Article 22.
[8] The UMA is the economic reference value in pesos used to calculate obligations and fines established in federal and state laws, as well as in the legal provisions derived from them

Do covered entities need to conduct Privacy Impact Assessments (PIAs)?

The LFPDPPP introduces formal data retention periods and mechanisms to block data prior to deletion. While explicit Privacy Impact Assessments (PIAs) are not referenced, the law's requirements for safeguards, breach notification, and mitigation imply a need for regular risk assessments and implementation of best privacy practices.

How Does Autodesk Comply with these Laws?

Autodesk has incorporated its disclosure and individual rights obligations into its global privacy program. For more information, including information on how individuals can exercise their rights under pertinent Privacy Laws at Autodesk, please see Autodesk's Privacy Statement and Autodesk's Trust Center Privacy page.