

A blue-toned background image featuring a globe in the center, surrounded by binary code (0s and 1s) and faint, glowing lines that suggest a digital or data environment.

Personal Data Held by Government Agencies Now Heavily Protected in Mexico

IN SHORT

The Situation: Mexican law did not hold government agencies to the same standards of personal data protection expected from private parties.

The Action: Enacted in January 2017, Mexico's General Law on the Protection of Personal Data Held by Regulated Subjects established specific procedures to protect private information held by government entities.

Looking Ahead: Mexican citizens are now able to enforce their so-called "ARCO Rights," and companies engaged in business with Mexican authorities should make sure they understand the protections required when working with personal data.

On January 27, 2017, Mexico's General Law on the Protection of Personal Data Held by Regulated Subjects ("Law") became effective. The Law establishes procedures to protect personal data held by government agencies and other public institutions. Up until this year, only private individuals and companies were adequately bound to establish data protection procedures.

In 2010, Mexico enacted the Federal Law on the Protection of Personal Data Held By Private Parties to protect personal data processed by private individuals and entities. Government agencies and entities did not have the same level of data protection obligations, creating a great disparity between the private and public sector. The Law brings balance and transparency to government action by providing the basis, principles, and procedures to guarantee the right of any data owner to the protection of his or her personal data under governmental control. The Law reiterates the constitutional principle that private communications are inviolable and that their intervention can be authorized only by federal judicial authority.

“ These changes certainly come in the right moment due to the increase in breaches of public records, such as the 2016 massive data breach that exposed voter records containing personal data of nearly 93.4 million Mexicans. ”

Data controllers, or "Regulated Subjects" under the Law, include any federal, state, or municipal authority, entity, organ, or body of the executive, legislative, and judicial branch of the government; autonomous bodies; political parties; and public trusts and funds. While federal entities already have some level of protection in place, most states, municipalities, and other public institutions such as political parties lack proper controls.

Regulated Subjects' new obligations include, among others, establishing mechanisms, security measures, and procedures for the protection of personal data, including comprehensive compliance programs and training.

Citizens will now be able to enforce their so-called "ARCO Rights"—rights to access, rectify, cancel, and oppose the processing of personal data held by Regulated Subjects, and to promote a revision recourse before the relevant transparency unit (within each Regulated Subject) or with the Mexican Data Protection Agency ("INAI") if they deem their rights have been violated. Personal data protection rights can be breached by Regulated Subjects only for reasons of national security, public order, safety, or public health and to protect third-party rights. The Law does not clarify the conditions for these exceptional cases to occur, thus these scenarios will be subject to judicial deliberation.

In the event of data security breaches— theft, loss, destruction, unauthorized access, or disclosure, among others—Regulated Subjects must analyze the causes and implement a work plan with preventive and corrective action. Data breaches that significantly affect financial or moral rights must be immediately notified to the relevant data owners, INAI, and other relevant bodies.

These changes certainly come in the right moment due to the increase in breaches of public records, such as the 2016 massive data breach that exposed voter records containing personal data of nearly 93.4 million Mexicans (the voter list belonged to a leftist political party that hired hosting services from an international company whose database was hacked). Now the Mexican Data Protection Agency can investigate hacking of government and political parties' databases involving theft of personal data and sanction the offenders.

The Law mandates the creation of a National Data Protection Program, which will entail an important process of harmonization throughout Mexico in order to adapt federal and local regulations to the general standard of the Law. Governments will need to classify and organize information in adequate forms.

Companies doing business with Mexican government institutions should have a clear understanding of the level of protection required for handling personal data exchanged and/or collected from government agencies or entities and the risks of entering into agreements or other programs with the government. As an example, health care companies and hospitals exchanging clinical files related to medical treatment provided by public health institutions such as IMSS (the Mexican Social Security Institute) and ISSSTE (the Institute for Social Security and Services for State Workers) will be subject to the new provisions. Data transfers must abide by the new rules and procedures for the protection of data under the Law. Individuals and entities interacting with the government must question the legality of the collection and use of any such personal data:

- Did the government agency obtain the consent of the data owner for the transfer?
- Can the company legitimately keep the data or share it with subcontractors?

There will be opportunities for companies to provide related services, such as IT services, cloud computing infrastructure, software, systems, controls, and protocols, to Mexican government agencies that can help Mexican Regulated Subjects comply with the new provisions.

FOUR KEY TAKEAWAYS

1. Mexico's new Federal Law on the Protection of Personal Data Held by Private Parties holds government entities to higher standards of personal data protection.
2. "Regulated Subjects" are responsible for a number of obligations to ensure compliance with the new law, and in the event of a security breach, they must implement a plan with preventive and corrective actions.
3. Companies conducting business with Mexican government institutions (for example, health care providers) should ensure that they are prepared for

"Regulated Subjects" OR "Data Controllers" Under the Law Include:

- Any federal, state, or municipal authority, entity, organ, or body of the executive, legislative, and judicial branch of the government;
- autonomous bodies;
- political parties; and
- public trusts and funds



CONTACTS



Mauricio F. Paez
New York



Guillermo E. Larrea
Mexico City

Mónica Peña, an associate in the Mexico City Office, assisted in the preparation of this Commentary.

the potential risks of handling private information.

4. IT implementation and support, cloud computing infrastructure, software, and similar services will be needed to assist Mexican Regulated Subjects comply with the new regulations, potentially creating significant opportunities for suppliers and vendors in these areas.

YOU MIGHT BE INTERESTED IN: [Go To All Recommendations >>](#)

\$2.5 Million Settlement Reached as HIPAA Crackdown Continues on Unsecured Portable Devices	Data Breach Risks for 401 (k) and Retirement Plans	Global Privacy & Cybersecurity Update Vol. 13	New Mexico On the Brink of Passing Data Breach Notification Law
---	--	---	---

SUBSCRIBE

SUBSCRIBE TO RSS



Jones Day is a legal institution with more than 2,500 lawyers on five continents. We are One Firm WorldwideSM.

Jones Day publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.

© 2017 Jones Day. All rights reserved. 51 Louisiana Avenue, N.W., Washington D.C. 20001-2113