Galicia

TMT Update

Publication of the Technical Manual for the Technological Solution for Diverse Institutions

Mexico City, January 28, 2026

On January 23, 2026, the "Technical Manual for the Technological Solution for Various Institutions" (the "Technical Manual") was published in the Federal Official, establishing the technical and cybersecurity requirements that private entities with databases containing personal data of any kind must meet in order to connect to the Single Identity Platform (PUI), a permanent, real-time consultation tool for searching and locating missing persons in Mexico.

Who does it apply to?

The scope of this definition is broad and potentially includes any private company that manages databases with personal information, explicitly including sectors such as finance, transportation, physical and mental health, telecommunications, education, private assistance, parcel and delivery services, employer and social security records, religious organizations, and addiction treatment.

This ranges from digital platforms, financial institutions, and hospitals to medical offices, private schools, human resources companies, and virtually any organization that stores personal data on customers, patients, students, or employees.

Main technical obligations

Complete development of technical infrastructure via APIs

- Development, maintenance, and security of proprietary API (application programming interface) endpoints, tailored to your needs and connected to the PUI;
- Backend server available 24/7 with fixed public IP and TLS certificates;
- Authentication system, active notification and continuous monitoring, as well as persistent searches for matches in local databases.

Indefinite continuous search

- Historical search of up to 12 years in databases;
- Permanent automated monitoring that periodically reviews new or modified records;
- The search ends only when the authorities close the report;
- Recurring operating costs with no time limit.

Three-phase search system

The system must allow for three phases of data search, basic and historical, including a mechanism for continuous and periodic search for possible matches.

Cybersecurity standards

Systems must be 100% free of vulnerabilities (critical, high, medium, and low) according to SAST/DAST/SCA reports. This standard requires:

- Business tools with high costs;
- Permanent specialized technical personnel;
- Operational, financial, specialized personnel, and maintenance challenges to implement and maintain it in production and operation 24/7 indefinitely.

The required cybersecurity and encryption standards are not necessarily the most suitable, nor are they those that might be currently used by companies and their policies and standards.

Responsibility for security and data

- Exclusive responsibility of the private sector for the security, availability, integrity, and confidentiality of systems; any leaks or vulnerabilities are the sole responsibility of the company;
- Obligation to share sensitive biometric data (photos, fingerprints) with specific encryption;
- Lack of clarity on compatibility with the Federal Law on Protection of Personal Data regarding consent and responsibility.

Penalties for non-compliance

Failure to provide access to records and databases may result in fines of between USD$68,000 and USD$136,160 (between MXN$1,173,100 and MXN$2,346,200) imposed by the Ministry of the Interior.

Broadly speaking, the Technical Manual transfers the costs of developing infrastructure, the risks in terms of data privacy and cybersecurity, as well as the responsibility and cost of carrying out this continuous monitoring to private entities.

Entry into force

The transitional provisions do not refer to the obligations of private entities. However, according to the Guidelines for the Development and Operation of the PUI, it is established that it will enter into operation 45 business days from the publication of three technical and operational manuals, two of which have already been published.

At Galicia, we can help you with support, from determining whether it applies to your company, the legal and technical implementation strategy, documentation and contracting of suppliers, privacy notices, among others.

Alternatively, we can explore with you the strategy for an *amparo*.

For further information, please contact Xavier Careaga (TMT & AI Counsel - xcareaga@galicia.com.mx).

* * *