RITCH MUELLER

July 29, 2026

DATA PRIVACY

CLIENT ALERT

SABG's Approach to Data Privacy Enforcement Following the FAN ID Decision

On July 12, 2026, the *Secretaría Anticorrupción y Buen Gobierno* (the "**SABG**"), Mexico's Ministry of Anticorruption and Good Governance, imposed a fine of **MXN$42,849,095** on the *Federación Mexicana de Futbol Asociación, A.C.* ("**FMF**") for violations of the Federal Law on the Protection of Personal Data Held by Private Parties (*Ley Federal de Protección de Datos Personales en Posesión de los Particulares(1)*, the "**LFPDPPP**") in connection with the processing of personal data through the **FAN ID** system.(2)

According to the authority's announcement, the SABG determined that the FMF: (i) failed to inform data subjects in its privacy notice that the photographs collected constituted sensitive personal data; (ii) obtained consent to process such data through a checkbox on a website, without implementing a mechanism capable of unequivocally evidencing the express and written consent required under applicable law; and (iii) failed to comply with the principles of lawfulness and accountability by not adopting the measures necessary to ensure the proper processing of personal data.

Although the decision may be challenged through the legal remedies available under Mexican law, it is one of the first public decisions in which the criteria applied by the SABG in exercising its supervisory and enforcement powers under the data privacy framework can be identified since it assumed the powers previously held by the now-defunct National Institute for Transparency, Access to Information, and Personal Data Protection (*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*; "**INAI**").

(1) Published in the Official Gazette of the Federation on March 20, 2025, together with its Regulations and other applicable provisions.
(2) https://www.gob.mx/buengobierno/prensa/buen-gobierno-sanciona-a-la-federacion-mexicana-de-futbol-con-42-8-millones-de-pesos-por-violaciones-a-la-proteccion-de-datos-personales?idiom=es

Key Implications

Beyond the amount of the fine, the decision provides relevant indications as to how the authority appears to be interpreting the obligations set forth in the LFPDPPP and the areas that are likely to receive particular scrutiny in future supervisory activities.

The authority's announcement and the conduct giving rise to the sanctions point to three areas of particular attention: (i) transparency regarding the processing of sensitive personal data; (ii) obtaining and retaining sufficient evidence of consent where legally required; and (iii) the effective implementation of compliance measures required under the accountability principle.

Notably, the decision did not arise from a security breach, unauthorized access or data leak. The sanctioned conduct primarily concerned how the data controller documented the processing of personal data and obtained consent from data subjects. This suggests that the authority's oversight will not be limited to investigating security incidents, but may also extend to ongoing compliance with the obligations set forth in the LFPDPPP.

In addition, although the authority's announcement does not provide the full reasoning underlying the decision, it is significant that the SABG found a violation of the principles of lawfulness and accountability in addition to the specific violations relating to the privacy notice and consent. If this approach is confirmed in future decisions, it could signal a broader interpretation of the accountability principle, under which the authority may assess not only the formal existence of policies and documentation, but also the effective implementation of governance and control measures throughout the personal data lifecycle.

Although the case involves biometric data, the obligations addressed by the authority extend beyond that particular context. Requirements relating to the content of privacy notices, obtaining consent, implementing security measures and complying with the accountability principle apply to any organization that collects, uses, stores or transfers personal data in Mexico. The processing of biometric data, however, raises the applicable level of scrutiny because such data constitutes sensitive personal data.

Matters Companies Should Review

In light of this precedent, organizations should consider reviewing, among other matters, the following aspects of their privacy compliance programs:

Area	Questions to Consider
Privacy notices	Does the company's privacy notice accurately identify the categories of personal data processed and expressly distinguish sensitive personal data where applicable?
Consent	Can the company demonstrate, through verifiable evidence, express and written consent where required by law?
Digital processes	Do the company's platforms, applications and electronic forms implement appropriate mechanisms to document consent and retain evidence of such consent?
Sensitive data	Is the processing of biometric, health or other sensitive personal data necessary, and are the appropriate legal and operational safeguards in place?
Governance	Are there policies, procedures, records, training programs and oversight mechanisms that allow the company to demonstrate compliance with the accountability principle?
Service providers	Do agreements with data processors and technology providers adequately address data protection and information security requirements?

Scope of Potential Sanctions

The LFPDPPP provides for fines calculated by reference to the *Unidad de Medida y Actualización* ("**UMA**")(3) , a statutory unit used in Mexico to calculate fines and other legal amounts, which may be doubled when the violations involve sensitive personal data.

Type of violation	Approximate exposure
Violations relating to privacy notices	Up to **MXN $18.7 million**
Insufficient consent and other more serious violations	Up to **MXN $37.5 million**
Potential doubling when sensitive personal data are involved	Up to **MXN $75 million**

(3) The UMA value in Mexico for 2026 is MXN $117.31 per day.

The fine imposed in this case, which was approximately **MXN$43,000,000**, demonstrates that the authority is prepared to impose significant sanctions where it identifies violations relating to the processing of sensitive personal data.

It also serves as a reminder that regulatory exposure does not depend solely on the existence of a security breach or personal data incident, but may also arise from non-compliance with structural obligations relating to transparency, consent and accountability.

Final Considerations

Although the full text of the decision will need to be reviewed to assess the SABG's reasoning in greater detail, this precedent provides insight into some of the criteria the authority has applied in exercising its supervisory and enforcement powers in the area of data privacy.

Against this backdrop, organizations should consider periodically reviewing whether their current data processing practices, as well as the documentation supporting those practices, accurately reflect how their operations, digital platforms and internal processes function in practice. Compliance programs often evolve at a different pace from business operations, which may create gaps between existing documentation and actual practices.

This decision serves as a reminder that data privacy compliance should be viewed as an ongoing process rather than a merely documentary exercise. As the SABG continues to develop its interpretation and application of the LFPDPPP, organizations should expect increased scrutiny of how they implement and document their privacy compliance programs.

We invite you to reach out to your usual contacts at Ritch Mueller to discuss any matter related to the issues described in this note.

Pablo Perezalonso Eguía
Partner
pperezalonso@ritch.com.mx
+52 (55) 9178 7050

Ricardo Calderón Mendoza
Partner
rcalderon@ritch.com.mx
+52 (55) 9178 7049

Isabel Ortiz Monasterio Borbolla
Senior Associate
iortizmonasterio@ritch.com.mx
+52 (55) 9178 7091