

FLASH LEGAL # 001200

The Superintendence for the Protection of Personal Data Reforms the Procedure for Filing and Processing Complaints and Requests and Issues the General Regulation on the Processing of Biometric Data

Dear Clients and Friends:

On September 24, 2026, two new resolutions issued by the Superintendence for the Protection of Personal Data (SPDP) were published in Official Register No. 376. The main elements of each resolution are summarized below:

1. Amendments to the Regulation on the Filing, Receipt, and Processing of Complaints and Requests (Resolution No. SPDP-SPD-2026-0038-R):

- **Exclusive digital channel:** Complaints and requests must be filed exclusively through the digital channel enabled on the SPDP's official website or through SISDPD using a valid electronic signature. A digitized handwritten signature will be accepted only on an exceptional basis.
- **Dismissal based on identity of cause:** If the reported facts have already been examined and processed in another complaint involving the same parties, subject matter, and cause, the complaint will be automatically dismissed and closed.
- **Use of AI as an auxiliary tool:** The SPDP authorizes and regulates the use of technological tools and artificial-intelligence agents to receive, classify, and analyze complaints and requests and to generate alerts and summaries. No decision producing legal effects may be based exclusively on the output of such technological tools without human assessment by a competent public official. Accordingly, the tool used and the official responsible for reviewing and validating its output must be recorded.

2. General Regulation on the Processing of Biometric Data (Resolution No. SPDP-SPD-2026-0039-R):

- **Scope of application:** The Regulation applies to the processing of biometric data for identification purposes obtained through automated, partially automated, or non-automated procedures. It classifies biometric data as sensitive personal data only where its processing is intended to uniquely identify a natural person.

Definitions: The Regulation introduces two relevant definitions:

- Raw biometric data: Biometric information captured directly from a natural person, including facial images, fingerprints, and any other biometric feature.
- Biometric template: A mathematical, encoded representation derived from raw biometric data and used to conduct biometric comparisons. The data controller must prioritize the use of biometric templates at all times and avoid storing raw biometric data, except where technically necessary.
- **Mandatory impact assessment**: Any entity that records and retains sensitive biometric data must conduct a risk assessment, which must be reviewed every 12 months. Enhanced security measures must be determined in accordance with the current version of the SPDP's Regulation on Risk Management and Data Processing Impact Assessments.
- **Enhanced consent requirements**: Consent must be prior, freely given, specific, informed, unambiguous, and explicit. The data controller must provide a non-biometric alternative, unless technical impossibility is duly documented. These requirements are heightened in contexts involving a significant imbalance of power, such as employment subordination, conditioning access to services or rights, or the absence of genuine alternatives.
- **Purpose limitation and necessity**: Biometric data may not be reused for purposes other than those that justified its original collection. Any additional purpose requires new consent. Before implementing a biometric system, the data controller must assess whether the intended objective can be achieved through other means. Biometric processing is permitted only where strictly necessary.
- **Prohibition of fully automated decision-making**: No decision producing legal effects or materially affecting an individual's rights may be based exclusively on automated biometric identification or on merely nominal human intervention. Data subjects have the right to request a reasoned explanation of the decision.
- **Prohibition of mass biometric systems in public spaces**: Mass biometric systems in public spaces are permitted only where expressly authorized by law and supported by a reasoned justification for the processing.
- **Facial recognition**: Facial-recognition systems must comply with Article 26 of the Organic Law on Personal Data Protection (LOPDP), as well as with the applicable risk-assessment and enhanced-security requirements. Their use does not constitute large-scale processing.

- **Minors:** The processing of biometric data relating to children and adolescents for identification purposes is prohibited unless no less intrusive means are available, an impact assessment has been conducted, and the explicit consent of the legal representative, guardian, or conservator has been obtained. Adolescents between 15 and 17 years of age may provide consent themselves, provided that the relevant information is presented in clear, age-appropriate language. Their legal representative may revoke that consent at any time.
- **Compliance period:** Data controllers currently using biometric systems have 12 months to bring their processes and systems into compliance with the Regulation.

We hope that you find this general information helpful. Please note that it is not intended to constitute legal advice. Should you have any specific inquiries, we would be pleased to provide further assistance.

NPTLegal
Abogados Ecuador

www.legalecuador.com

If you wish to unsubscribe from this type of information, please email us at: desuscribirse@legalecuador.com