BUSTAMANTE FABARA

Innovation and Legal Leadership in Ecuador

↗ **LEGAL** BULLETIN

New Resolutions Issued by the Superintendency of Personal Data Protection ("SPDP"): Amendments Regarding AI, Complaints and Requests; and New Rules on Biometric Data and Security Breaches

New Resolutions Issued by the Superintendency of Personal Data Protection ("SPDP"): Amendments Regarding AI, Complaints and Requests; and New Rules on Biometric Data and Security Breaches

On September 10, 2026, the SPDP made public four new key resolutions issued on September 9, 2026:

1. Resolution No. SPDP-SPD-2026-0037-R, which amends the General Regulation for Safeguarding the Right to Personal Data Protection in the Use of Artificial Intelligence Systems.
2. Resolution No. SPDP-SPD-2026-0038-R, which amends the Regulation for the Filing, Receipt, and Processing of Complaints and Requests.
3. Resolution No. SPDP-SPD-2026-0039-R, which issues the General Regulation for the Processing of Biometric Data.
4. Resolution No. SPDP-SPD-2026-0040-R, which issues the Technical Regulation on Notifications of Personal Data Security Breaches.

1. Resolution No. SPDP-SPD-2026-0037-R (Artificial Intelligence "AI" Amendment)

The amendment clarifies the scope of the obligations applicable to processors that have access to, visibility of, or effective control over personal data processed through AI systems. It also incorporates these categories as operational definitions to determine when a processor falls within the scope of the regulation.

Providers, developers, or maintainers of AI systems must provide the controller with sufficient information regarding their operation, limitations, foreseeable risks, and control measures, without disclosing trade secrets or intellectual property. These obligations will apply only to operations over which the processor has access, visibility, or effective control, and evidence must be retained when the processor claims that such conditions do not exist.

2. Resolution No. SPDP-SPD-2026-0038-R (Amendment on Complaints and Requests)

The amendment updates the definitions of complaint, request, and acknowledgment of receipt, and establishes the mandatory digital filing of these procedures through the SPDP website or through the system developed by the regulator, known as SISPDP. The forms must bear a valid electronic signature or, exceptionally, a digitized handwritten signature.

During preliminary proceedings, the investigated party will have 10 days to respond to the preliminary findings, while the administrative decision must be notified within a maximum period of 6 months.

3. Resolution No. SPDP-SPD-2026-0039-R (Biometric Data)

The regulation establishes conditions, safeguards, and limitations for the processing of biometric data. All processing must be preceded by a risk analysis and a Data Protection Impact Assessment ("DPIA"), which must be updated every 12 months.

When processing is based on consent, such consent must be prior, freely given, specific, informed, unambiguous, and explicit, and the data subject must be offered an alternative that does not require the use of biometric data.

Mass and indiscriminate identification in public spaces is prohibited, except where required by law, as is the reuse of biometric data for purposes other than those that justified its collection. Enhanced restrictions and

specific consent requirements are established for minors. Controllers that already use biometric systems will have 12 months to comply with the regulation.

4. Resolution No. SPDP-SPD-2026-0040-R (Security Breaches)

The regulation governs the notification and management of security breaches by controllers and processors. Breaches may affect confidentiality, integrity, and availability, while also taking into account criteria related to timing, permanence, and irreversibility.

Notifications must be submitted through SISPDP, and failure to notify will be considered a serious infringement under the LOPDP. The regulation also introduces AIxSPDP, an auxiliary expert system based on artificial intelligence and subject to human intervention, designed to facilitate traceability, metric generation, and risk analysis of notifications.

At **BUSTAMANTE FABARA**, we will continue to share specialized analysis on the practical application of these regulatory instruments and their implications for the different regulated sectors.

For further information, please contact:

- Dra. María Rosa Fabara: **mrfabara@bustamantefabara.com**
- Esteban Dávila: **edavila@bustamantefabara.com**
- Rafael Gabela: **rgabela@bustamantefabara.com**
- Marco Sánchez: **msanchez@bustamantefabara.com**