

TECHREG REGULATORY INTELLIGENCE.

Summary: ANPD steps back from its guide on high-risk data processing and signals a more integrated risk management approach.

WHY DOES IT MATTER?

On September 21, the Brazilian National Data Protection Authority (ANPD) decided not to approve and to archive, in its current form, the Guidance on High-Risk Personal Data Processing, bringing to a close a regulatory process that had been under development for several years.

The decision does not eliminate the concept of high-risk processing, nor does it reduce the obligations established under Brazil's General Data Protection Law (LGPD). Its main effect is different: at this stage, the ANPD has decided not to consolidate a specific and standalone methodology for defining and assessing high-risk situations.

The move is relevant because it signals a change in the Authority's regulatory strategy. Instead of addressing the concept of high risk in isolation, the Board of Directors indicated a preference for a broader risk-management approach, potentially integrated into the future regulation of Data Protection Impact Assessments (DPIAs).

For companies that develop or use artificial intelligence, automated decision-making systems, biometrics, emerging technologies, or large databases, the decision preserves an important degree of regulatory interpretation.

The key point is that the ANPD did not reject the need to identify high-risk processing activities. On the contrary, it acknowledged the relevance of the issue, but concluded that the proposed methodology was excessively complex and could fragment the Authority's broader risk-management policy.

In practical terms: the issue has been removed from a standalone guidance document, but it has not left the regulatory agenda.



WHO DOES IT MATTER TO?

The decision is particularly relevant for companies engaged in data-intensive activities or using technologies capable of producing significant impacts on individuals.

The sectors most exposed include:

- Artificial intelligence and technology companies, particularly applications that use personal data for training, personalization, or decision-making;
- Banks, fintechs, insurers, and credit companies, due to the use of automated systems for risk analysis, credit assessment, fraud detection, and profiling;
- Digital platforms, adtechs, and marketing companies, especially in profiling and behavioral advertising activities;
- Healthtechs, hospitals, laboratories, and pharmaceutical companies, due to the use of sensitive personal data;
- Companies using biometrics and facial recognition;
- Human resources companies and HR techs, when algorithms are used in recruitment, evaluation, or termination processes;
- Services directed at children and adolescents;
- Small and medium-sized companies using emerging technologies, which were among the main audiences originally targeted by the guidance.

The decision is especially relevant for companies currently building AI governance programs. Whether an operation is classified as high risk may determine additional governance, documentation, and assessment requirements.

WHAT DID THE ANPD DECIDE?

The Board of Directors reviewed the matter under Deliberative Circuit No. 25/2026, opened on September 11 and concluded on September 21, 2026.

Director Miriam Wimmer, rapporteur for the case, recommended that the Guidance on High-Risk Personal Data Processing not be approved and defended its archiving.

“Despite the relevance of the topic, the draft, as proposed, does not fully achieve the objectives it seeks to address, either because of the complexity of the proposed methodology or because the analysis focuses on only one of the aspects involved in risk management in personal data processing. It should be noted, for example, that although the methodology proposed for assessing large-scale processing

seeks to bring greater objectivity to the analysis of the elements that make up this criterion — volume of data, duration of processing, frequency, and geographic scope — it ends up introducing excessive complexity, making its day-to-day application by processing agents more difficult. This approach may not reflect the reality of companies, particularly micro, small, and medium-sized enterprises,” Wimmer stated in her vote.

The other three participating members of the Board fully supported the rapporteur’s position. The decision was therefore unanimous among the four votes recorded.

The guidance had been developed to help processing agents — especially smaller companies — identify situations considered high risk under LGPD regulation.

The regulatory process had gone through several stages:

2022 — call for input;

2023–2024 — drafting and revision of the first version;

April–May 2024 — public consultation;

2025 — assessment of contributions and legal review by the Specialized Federal Attorney’s Office;

September 2026 — final decision by the Board of Directors.

The Specialized Federal Attorney’s Office itself had considered publication of the guidance legally viable, subject to recommended adjustments. The decision not to publish it was therefore a **regulatory and methodological choice by the Board of Directors**, rather than the result of a legal impediment.

WHY WAS THE GUIDANCE REJECTED?

The rapporteur’s vote identifies two main concerns.

1. The methodology was considered excessively complex

The proposal sought to make certain criteria associated with high-risk processing more objective.

One example is the concept of **large-scale processing**. The proposed methodology considered factors such as:

- volume of data;
- duration of processing;
- frequency;

- geographic scope.

According to the vote, despite the attempt to introduce greater objectivity, the methodology could generate excessive complexity in day-to-day implementation.

The concern would be even greater for **micro, small, and medium-sized companies**, which were among the main intended users of the guidance.

2. Risk of regulatory fragmentation.

The second argument is particularly important for anticipating the ANPD's future regulatory strategy.

The rapporteur considered that publishing a document focused exclusively on high-risk processing before establishing a broader approach to risk management could result in fragmented regulation.

According to the vote, it would be preferable to address the concept of high risk together with other elements of risk management, particularly within the framework of **Data Protection Impact Assessments — DPIAs**.

This points to a possible shift in regulatory architecture:

Standalone guidance on high-risk processing.

↓

Integrated system for risk identification, assessment, documentation, and mitigation.

WHAT CHANGES FOR COMPANIES?

In the short term, **the decision does not create any new obligation**.

It would also be incorrect to interpret the archiving of the guidance as a relaxation of the high-risk concept.

Existing rules remain in force.

Until there is specific regulation on DPIAs, the ANPD continues to advise controllers, where applicable, to use the criteria established in ANPD Resolution No. 2/2022 to assess high-risk processing activities.

Under this framework, processing may be considered high risk when it combines at least:

one general criterion, such as:

- large-scale processing; or

- processing capable of significantly affecting fundamental interests and rights;

with one specific criterion, such as:

- use of emerging or innovative technologies;
- surveillance or monitoring of publicly accessible areas;
- decisions made exclusively on the basis of automated personal data processing;
- use of sensitive personal data;
- use of data concerning children, adolescents, or elderly individuals.

For companies using AI, the discussion therefore remains directly relevant.

IMPACT ON ARTIFICIAL INTELLIGENCE.

The decision deserves particular attention from companies developing or implementing AI systems.

This is because two elements already present in the current regulatory framework connect directly with artificial intelligence applications:

emerging or innovative technologies; and

decisions made solely on the basis of automated processing of personal data.

The use of AI, by itself, does not automatically make every data-processing activity high risk.

However, when AI systems are deployed at scale or produce significant effects on individual rights — in areas such as credit, employment, healthcare, education, insurance, or access to services — the need for risk assessment and documentation of safeguards increases substantially.

The trend signaled by the ANPD's decision is that this analysis will be incorporated into a broader governance and risk-management framework, rather than being limited to a standalone checklist for classifying high-risk activities.

DATA PROTECTION IMPACT ASSESSMENTS GAIN IMPORTANCE.

The most important element of the vote for anticipating the ANPD's next regulatory steps is the connection between high-risk processing and Data Protection Impact Assessments.

A DPIA is the document in which the controller describes processing activities that may create risks to the rights and freedoms of data subjects, as well as the safeguards and mechanisms adopted to mitigate those risks.

The ANPD recommends preparing a DPIA whenever an operation may involve high risk and may formally require such an assessment in certain circumstances.

By rejecting the guidance, the rapporteur suggested that the discussion on high risk should be incorporated into the future regulatory development of DPIAs.

This means that **DPIAs are becoming one of the main regulatory monitoring points for data-intensive and AI-driven companies.**

WHAT DOES THE DECISION SIGNAL?

TechReg's assessment is that the decision reveals three important developments.

First: the ANPD is avoiding, at this stage, an overly prescriptive methodology for classifying risk.

Second: there is a shift toward a more integrated **risk-management model**, combining identification, assessment, documentation, mitigation, and accountability.

Third: companies will continue to bear significant responsibility for conducting their own risk assessments while the Authority has not yet consolidated additional criteria.

The ANPD's current guidance itself recognizes that risk-management methodologies may vary and that controllers are responsible for assessing the specific circumstances of each processing activity, the potential impacts on data subjects, and the corresponding preventive measures.

NEXT STEPS.

The Superintendence of Regulation is expected to assess whether parts of the studies and methodology developed during preparation of the guidance may be reused in future regulatory work. This possibility was expressly acknowledged by the Board of Directors.

The ANPD's Regulatory Agenda currently lists the high-risk data-processing project as **closed**, following the process that resulted in the guidance being archived.

For companies, monitoring should now shift toward:



1. Regulation of Data Protection Impact Assessments;
2. New documents on risk-management methodologies;
3. ANPD enforcement involving processing activities considered high risk;
4. Decisions involving automated systems and artificial intelligence;
5. Interaction between the LGPD and Brazil's future artificial intelligence regulatory framework.

TECHREG ASSESSMENT.

Immediate regulatory impact: Low.

Strategic impact: High.

Time horizon: Medium term.

Most exposed companies: AI, technology, digital platforms, financial services, healthcare, biometrics, HR tech, digital advertising, and companies processing data concerning children and adolescents.

The decision does not create new obligations, but it provides an important signal as to **how the ANPD intends to build its future risk-management architecture.**

For companies using artificial intelligence, the main risk would be to interpret the archiving of the guidance as a reduction in regulatory pressure.

The signal appears to point in the opposite direction: **the ANPD is reconsidering how risk should be regulated in order to build a broader and more integrated model.**

TECHREG MONITORING.

TechReg will continue to monitor decisions by the ANPD Board of Directors, the future regulation of DPIAs, initiatives related to artificial intelligence, and the evolution of the criteria used by the Authority to define high-risk processing.

For companies using personal data in artificial intelligence systems, anticipating these definitions will be increasingly relevant to building governance, compliance, and risk-assessment frameworks before the next regulatory obligations are consolidated.

TECHREG REGULATORY INTELLIGENCE.

