

PUBLIC CONSULTATION: PRELIMINARY STUDY ON HIGH RISK AND LARGE SCALE

The National Data Protection Authority (ANPD) opened a **public consultation regarding the Preliminary Study on High Risk and Large-Scale processing** of personal data. Contributions can be made through the Participa+Brasil platform. The Preliminary Study includes a draft **Guidance** on high-risk processing of personal data, as well as a suggested **risk calculation methodology** developed by the ANPD.

Published: 17/04/2024

Closure: 16/05/2024



Goals

The purpose of the Preliminary Study is to elucidate the concept of high risk in order to provide guidance for its proper identification by data controllers, promoting greater legal certainty and transparency.

The Preliminary Study outlines the criteria that data controllers should take into account and provides several examples of using the methodology recommended by the ANPD – which is also applicable in situations involving the assessment of the need for notification of a security incident involving personal data.

HIGH-RISK PROCESSING

The processing of personal data will be considered high-risk when it cumulatively meets at least (i) one **general criterion** and (ii) one **specific criterion**:

General criteria



Large-scale processing



Processing that may significantly affect the interests and rights of data subjects



Specific criteria



Surveillance or control of publicly accessible areas



Automated data processing



Emerging or innovative technologies



Sensitive data or data of children, adolescents, or the elderly

General criteria

1 Large-scale processing

The large-scale characterization involves several elements:

Main Element



Number of data subjects

With the rationale of promoting greater legal certainty and transparency, the ANPD defines “on a large scale” any processing that involves at least 2 million data subjects*.

IMPORTANT: if the processing involves this quantity of data subjects, the large-scale criterion will be configured, regardless of the assessment of the complementary criteria below.

*approximately 1% of the Brazilian population according to the 2022 Census.

Complementary Elements



Volume of data involved

It corresponds to the total number of personal data records processed divided by the number of data subjects.



Duration of data processing

It refers to the time interval during which personal data are processed for a specific purpose – from data collection to disposal. In this case, the shorter the period of data processing, the lower the impact for the purposes of large-scale characterization – and vice versa.



Frequency of processing

It refers to the rate of repetition of data processing. According to its methodology, the ANPD defines a scale that ranges from: multiple occurrences daily; daily; weekly; monthly; or annually.



Geographical extent of processing

It refers to determining the scope and reach of processing operations. The greater the scope of data processing, potentially covering different regions, the greater the impact.

The ANPD proposes a calculation formula to assess these elements, considering the assignment of weight to each of them. Ultimately, the goal of the calculation is to determine whether the activity involves large-scale data processing or not.

2 Processing that may significantly affect the interests and rights of data subjects

While “large-scale” presupposes a quantitative analysis, the second general criterion has a qualitative character: it refers to the magnitude of the impact that the processing of personal data activity can represent on the interests and fundamental rights of data subjects. For this purpose, the ANPD points to the need to consider 3 elements:



Impediment to the exercise of rights

When the processing activity prevents the exercise of rights guaranteed by the Constitution, laws, or regulations – for example, the right to access information, the right to freedom of expression, or the right to non-discrimination.



Preventing the use of an essential service

When the processing activity represents an impediment to access the offer of goods or services in physical or digital environments, whether for profit or not, such as the sale of products, financial services, social assistance services, among others.

IMPORTANT: This element does not include legitimate refusals to provide a service, such as when the data subject fails to make the corresponding payment.



Moral or material harm to data subjects

When the processing activity causes financial losses or non-economic damages to the data subject – such as those affecting their reputation or image, causing humiliation, embarrassment, or psychological distress.

IMPORTANT: This also includes potential situations, so it is not necessary for the harm to materialize.

Specific criteria

1 Emerging or innovative technologies

The ANPD defines emerging technologies as those with the **potential to shape or reshape business models and exert significant influence on the economy**. These are innovations with practical applications, a high degree of commercial interest, and the potential for rapid growth and impact on society.

By considering the “use of emerging and innovative technologies” as a specific criterion for assessing high risk, the ANPD requires data controllers to analyze, based on the state of the art and technological development, whether a particular technology falls into this category.

The ANPD cites examples such as: (i) AI, machine learning, and generative AI; (ii) facial recognition systems; and (iii) autonomous vehicles.

2 Surveillance or control of publicly accessible areas

This criterion assesses processing activities aimed at monitoring or controlling the presence and circulation of people in public or privately accessible areas, such as streets, squares, metro stations, airports, stadiums, shopping centers, etc. The ANPD cites examples such as the use of security camera systems, monitoring drones, and GPS.

IMPORTANT: Exclusive use in a domestic environment does not characterize this specific criterion.

3 Automated data processing

This criterion involves the use of computational systems and algorithms to perform operations or make decisions related to personal data, including preclassification, evaluation, approval, or rejection based on predefined criteria.

The sensitivity of the criterion refers to the possibility of automated decisions posing risks to individual rights and freedoms, such as algorithmic discrimination and the possibility of discrimination through unfair generalization.

IMPORTANT: The ANPD emphasizes that this criterion applies only to significantly automated data processing.

4 Sensitive data or data of children, adolescents, or the elderly

The ANPD advocates for this criterion because these categories of data require a higher degree of protection.

For sensitive data, the definition provided by the LGPD should be considered; for children and adolescents, the definition from the Statute of the Child and Adolescent prevails (a child is a person up to 12 years of age, and an adolescent is someone between 12 and 18 years old); whereas for the elderly, it is necessary to consider the Statute of the Elderly (a person aged 60 years or older).

IMPORTANT: The ANPD emphasizes that the list provided in Article 5, II, of the LGPD, related to sensitive data, is exhaustive.

/ Insights b/luz

Once again, ANPD demonstrates its commitment to enhancing the regulation and interpretation of key aspects of the LGPD. By releasing this Preliminary Study, the Authority seeks to clarify points that may generate controversies and uncertainties, particularly regarding the risk of processing activities and the possible classification into specific regimes, including those applicable to small-scale processing agents. This initiative signals the ANPD’s concern to ensure a more precise and uniform application of data protection rules, thereby contributing to greater legal certainty.

