



June 28, 2021

Waldemar Gonçalves Ortunho Junior
President, Board of Directors
National Data Protection Authority

Re: ANPD Consultation on Enforcement and Sanctions

BSA| The Software Alliance (BSA) welcomes the opportunity to provide feedback to the National Data Protection Authority (Autoridade Nacional de Proteção de Dados - ANPD) on the draft resolution to provide for the enforcement and application of sanctions (Draft Resolution) regarding the Brazilian Personal Data Protection Law (LGPD).

BSA supports data protection rules that are risk-based, technology neutral, and flexible. BSA members have a deep and long-standing commitment to protecting their customers' data across technologies and business models. We also recognize that to be effective, a privacy regulator needs appropriate tools and must ensure that remedies imposed on entities that violate the data protection law are proportionate to the harm resulting from violations. We commend the ANPD for its efforts to develop enforcement regulations that promote an evidence-based approach, transparent and fair processes, and proportionality between risks and allocated resources.

Our comments address three aspects of the Draft Resolution, focusing on the need to ensure: (1) effective regulatory tools, (2) remedies that are proportionate to harms caused by violations, and (3) regulations that promote privacy, without inadvertently creating privacy and security risks.

I. Need for Effective Regulatory Tools

Data Protection Authorities should have the tools and resources necessary to ensure effective enforcement of national data protection laws. The ANPD's ability to effectively enforce the LGPD is critical to protecting individuals' privacy, ensuring that organizations subject to the law meet their commitments and legal obligations, and deterring potential violations. The LGPD establishes a number of remedial tools and authorities for the ANPD, to ensure it can carry out this mission. We offer views on the Draft Resolution's treatment of two such tools:

- **Supervision Premises.** The Draft Resolution sets out a range of premises on which the ANPD will base its supervisory activity, including prioritizing actions based on evidence and risk

management, adopting measures that are proportional to identified risks, and encouraging the promotion of a culture of protection of personal data. We believe these premises are critical to the work of any regulator, and strongly support the ANPD's recognition that its activities should focus on evidence of actual practices and risks of harms created by violations.

- **Mapping of Priorities.** The Draft Resolution also anticipates that the ANPD will conduct a biennial mapping of priorities that will enable the regulator to prioritize its activities and resources. We support this approach, which creates a structure for implementing the ANPD's evidence-based and risk-based method of regulation. At the same time, the Draft Resolution does not appear to contemplate a role for stakeholder consultation in connection with this mapping. However, stakeholder feedback may help the ANPD refine its priorities and understand concerns that may not clearly arise through the agency's monitoring cycle or elsewhere – including emerging issues that are not yet reflected in evidence gathered by the regulator. *We therefore urge the ANPD to consider amending Articles 20-22, to create a mechanism for the ANPD to solicit stakeholder feedback on draft biennial mappings (via a public consultation) before each of those mappings are finalized.*

II. Need for Remedies to be Proportionate to the Harm Resulting from Violations

Effective remedies in a data protection framework are important to ensuring that individuals' rights are sufficiently protected and companies are deterred from violating their obligations under the law. However, it is important to structure remedies and penalties to be effective and proportionate to the harm resulting from those violations. We appreciate the Draft Resolution's approach to ensuring the ANPD applies remedies that are proportionate to violations, in an evidence-based manner.

We offer views on three such aspects of the Draft Resolution:

- **Clear and Distinct Ranges of Enforcement Options.** We strongly support the Draft Resolution's approach to setting out clear and distinct ranges of enforcement options, including several options that may be used without imposing sanctions. This ensures the ANPD has a broad set of enforcement options to consider in determining which remedy is appropriate given the facts of a particular case. Specifically, the Draft Resolution recognizes that in certain cases the appropriate remedy will be to issue guidance, apply preventative measures, request regularization, or enter into a compliance plan – and that these options may be appropriate when the application of sanctions is not the proportionate remedy. These options recognize that in many cases, companies that are informed or warned their conduct may be in violation of the law will correct their conduct voluntarily and provide companies with strong incentives to do so. At the same time, the Draft Resolution appropriately recognizes the ANPD's ability to seek monetary penalties when companies do not take appropriate measures in a timely manner.
- **Case-Specific Fact-Finding.** The Draft Resolution also recognizes that enforcement decisions will be based on the criteria set out in the LGPD, which provides that any sanction must be imposed in accordance with the "peculiarities of the particular case" and must take into account criteria including the severity and nature of the infraction, the good faith of the offender, the advantage received or intended by the offender, the economic condition of the offender, recidivism, the level of damage, the cooperation of the offender, adoption of internal procedures capable of

minimizing damage, adoption of good governance policy, the prompt adoption of corrective measures, and the proportionality between the severity of the breach and the intensity of the sanction. (See Draft Resolution Section III, citing LGPD Article 52.) The Draft Resolution states that a decision is to be “motivated” by these criteria, without also expressly stating that the criteria set out in the LGPD will be specifically referenced in the ANPD decisions. We believe the Draft Resolution should more expressly reference the LGPD’s criteria, both to highlight that those criteria will be embedded into the ANPD’s underlying processes and to create clear incentives for companies to adopt good governance policies and practices in line with those criteria. We therefore urge amending Article 61 of the Draft Resolution to require the ANPD to clarify that ANPD’s written decisions will make express reference to each of the LGPD Article 52 specific criteria, which would not only heighten the focus on these required criteria but also increase transparency as to how the agency considers and weighs those criteria.

- **Timelines in Enforcement Actions Should Allow for Case-Specific Fact Finding.** Finally, we note concerns with the short timeframes for responding to several aspects of the ANPD’s sanctions process. For example, Article 53 anticipates that companies will present a defense within 10 days of receiving a summons; Article 59 provides 10 days to respond to final allegations, and Article 64 anticipates an appeal will be filed within 10 days. These short timeframes have the potential to prevent companies from assembling the full set of factual information relevant to the ANPD’s inquiry and could limit the agency’s ability to understand the factual context for any alleged violation. As a result, these short timelines could hinder the ANPD’s ability to ensure a remedy is proportional to the particular facts of a given case. We urge ensuring the sanctions process contains flexibility in these timelines, by both creating a default time frame that is longer than 10 days and by ensuring that companies may seek an extension of those timeframes in appropriate cases.

III. Ensure Remedies Are Not Administered in a Manner That Undermines Privacy or Security

The Draft Resolution also sets out a range of duties imposed on companies that are subject to the ANPD’s jurisdiction. While we share the goal of ensuring those obligations preserve the privacy of personal data subject to the LGPD, we highlight two concerns with the current language, which could inadvertently undermine privacy and security-protective practices.

- **Potential for On-Site Audits.** In Article 5, the Draft Resolution provides that companies are to allow the ANPD access to facilities and equipment for the evaluation of their personal data processing activities. While we recognize the need for companies to provide appropriate information to the ANPD in the course of an enforcement action, on-site audits such as those contemplated by Article 5 can raise specific security and privacy concerns, particularly when the company at issue may provide business services to a wide range of other companies whose activities are not the focus of inquiry. For example, an on-site audit of a company acting as a service provider for dozens or hundreds of customers may expose the on-site auditing team to a range of information that is not the subject of their efforts, unless the regulator and the company work to implement privacy and security safeguards regarding how information is to be reviewed on site. In the context of cloud services, for example, on-site audits often provide very

little information beyond that available through other sources, because the data most relevant to an investigation may simply need to be collected from servers – and is more efficiently reviewed and analyzed off-site rather than on the provider’s premises. We therefore urge Article 5 to be revised to recognize that the ANPD should limit the use of on-site audits and should take steps to address privacy and security concerns that may be raised by an on-site audit in a particular instance.

- **Data retention.** Similarly, Article 5 also requires companies to retain physical and digital documents for the time periods established in the LGPD, as well as throughout the period of processing for administrative processes in which they are necessary. If read broadly, this language could inadvertently create privacy and security risks by incentivizing companies to retain data they otherwise would not, including data for which there may not be a business need to retain. This creates privacy and security risks because the data remains accessible to some set of actors at that point, rather than being securely deleted or de-identified. We urge the ANPD to clarify that Article 5 does not impose any data retention obligations additional to those contained in the LGPD and other existing laws.

* * *

BSA appreciates the ANPD’s solicitation of feedback on the Draft Resolution and would be pleased to serve as a resource as development the resolution continues.

Sincerely,

BSA | The Software Alliance