September 15, 2022

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

Re: Regulation of Dosimetry and Application of Administrative Penalties

BSA | The Software Alliance (BSA)[1] welcomes the opportunity to provide feedback to the National Data Protection Authority (Autoridade Nacional de Proteção de Dados - ANPD) on the draft resolution approving the Regulation of Dosimetry and Application of Administrative Penalties (Regulation) under the Brazilian Personal Data Protection Law (LGPD).

BSA is the leading advocate for the global software industry. Our members are business-to-business companies that create the technology products and services that power other companies, including cloud storage services, customer relationship management software, identity management services, and workplace collaboration software. BSA members invest significantly in privacy and security, and they have made protecting the privacy of their customers' data a top priority.

BSA supports data protection rules that are risk-based, technology neutral, and flexible. We also recognize that to be effective, a privacy regulator needs sufficient enforcement tools and must impose appropriate remedies on entities that violate the data protection law. We commend the ANPD for its efforts to develop enforcement regulations designed to reduce complexity and create a transparent and fair process with a range of possible remedies.

As sanctions are assessed, a key consideration should be whether the sanction is proportionate to the risk of harm resulting from law violations. Our comments focus on better achieving this balance in three aspects of the Regulation: (1) ensuring appropriate criteria for the classification of infractions; (2) assigning appropriate weight to aggravating and mitigating factors; and (3) articulating more specific criteria for severe non-monetary sanctions. These recommendations can help to create a reliable baseline for the imposition of sanctions by creating a clear set of risk-based penalties that are proportionate to the harm they are meant to address.

[1] BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Prokon, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

I. Criteria for Classification of Infractions

Article 8 of the Regulation identifies three different categories of infractions: light, medium, and serious. These categories establish the foundation for calculating the base value for penalties for violations of the LGPD. We support the ANPD's efforts to apply graduated sanctions based on different classes of violations, but we encourage the ANPD to revise the criteria for these classifications so that they appropriately target activities that pose substantial risks of harm and provide sufficient notice of the proscribed conduct.

- **Medium Infractions.** The Regulation provides that a medium designation will be applied if the infraction involves large-scale processing or significantly affects the fundamental rights of the holder. This standard could allow a medium designation solely because of large-scale processing, even in circumstances where the underlying infraction poses minimal risks.

  We strongly recommend designations focus on the risks associated with the actual infraction, rather than the scale of the associated processing. The Regulation indicates that considerations for determining whether there is large-scale processing of personal data include a significant number of data subjects, the volume of data involved, and the duration, frequency, and geographical extent of the processing performed. Applying this standard, the Regulation could be read to treat every global company that does business in Brazil as always having, at a minimum, a medium-level infraction since the factor for this classification is based solely on the fact that large-scale processing occurs, rather than the risks created by the specific infraction. For example, the privacy risk associated with an incident may be minimal because it involved encrypted information, yet the heightened classification could nonetheless be read to apply when there is large scale processing. *We urge the ANPD to modify the basis for a medium classification so that it effectively implements a risk-based approach to enforcement*.

- **Serious Infractions.** The Regulation provides that the serious classification applies, among other things, if the entity obtains or intends to obtain an economic advantage as a result of the infraction. This formulation appears to go beyond the LGPD's contemplation of the advantage obtained by the sanctioned entity, and could be construed broadly to extend the serious classification to any entity conducting business merely because its use of data happens in a commercial context. This should not be the basis for a serious classification. Rather, the most serious classification should address egregious circumstances.

  Under the regulation, the serious classification also applies if the "infringer prevails on the weakness or ignorance of the holder, in view of his/her age, health, knowledge or social condition." This standard is vague and does not sufficiently identify the circumstances that trigger its application. If read broadly, it could include circumstances where there is unequal bargaining power, which could happen whenever a corporate entity is interacting with an individual. It also is not clear what evidence is sufficient to demonstrate knowledge of an individual's age, health, knowledge, or social condition and, even where there is demonstrable knowledge, that there was an intent to take advantage of the individual based on those factors. If the ANPD aims to address different circumstances involving bad faith, this requirement should be made explicitly in the text.

  We urge the ANPD to eliminate these two factors for categorizing an infraction as serious and, if they are not deleted altogether, modify them to be more specific so that the ANPD can sufficiently target egregious conduct that warrants stricter penalties.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

II. Assigning Appropriate Weight to Aggravating and Mitigating Factors

Articles 14 and 15 of the Regulation delineate aggravating and mitigating factors to consider when calculating a simple fine. We appreciate the ANPD's efforts to identify conduct appropriate for increasing or reducing a fine. To implement a risk-based approach effectively, the ANPD should reduce the proposed fine increases for aggravating factors and, conversely, accord more weight to the mitigating factors. The ANPD should also ensure that all mitigating factors are considered when applying sanctions in individual cases.

- **Aggravating Factors.** The Regulation applies a 20% increase in a simple fine for failing to comply with preventive measures during the inspection process or preparatory procedure, but the ANPD can increase the fine up to 80%. Similarly, the Regulation applies a 30% increase in the fine for not complying with corrective measures, and this can be increased up to 90%. These maximum allocations for fine increases are excessively harsh. The aggravating factor could, by itself, almost double the fine. The Regulation also does not require these fines be commensurate with the seriousness of the underlying infraction. *We urge the ANPD to reduce the maximum percentages for fine increases based on aggravating factors to ensure the sanction is proportionate to the harm.*

- **Mitigating Factors.** In contrast, the ANPD should increase the weight assigned to mitigating factors to further reduce fines where there are efforts to minimize harm. We support the fine reductions for cessation of infractions, however, the Regulation assigns minimal weight to other mitigating factors. The Regulation reduces the fine by 20% if an entity implements a governance policy or otherwise adopts internal mechanisms capable of minimizing the damage before the first decision is rendered during the administrative sanctioning process. The Regulation also reduces the fine by 20% when a sanctioned entity has proven the implementation of measures capable of reverting or mitigating the effects of the violation prior to the initiation of the preparatory procedure or administrative sanctioning procedure. The Regulation reduces the fine —by only 5% — where there is cooperation or good faith.

  Importantly, good faith and cooperation are key to ensuring compliance, and these factors create strong incentives for companies interacting with the ANPD. These factors accordingly merit more fulsome consideration for purposes of mitigating an infraction. Moreover, because the maximum percentages are so high for the aggravating factors, there is no parity with the percentage of reductions for the mitigating factors. If failure to comply with a corrective measure can lead to an 80% or 90% increase in fine, implementing internal measures that minimize the risk of harm should have a substantial impact on the fine as well—larger than 20%. *We urge the ANPD to increase the amount that fines are reduced for mitigating factors related to good faith, cooperative actors, and implementation of governance policies or other internal measures that minimize risk of harm*.

- **LGPD Article 52 factors.** Article 7 of the Regulation identifies the factors enumerated in Article 52 of the LGPD, recognizing that the ANPD takes them into account when defining the parameters of the sanctions. These factors are:
  - the severity and the nature of the infractions and of the personal rights affected;
  - 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 mechanisms and procedures capable of minimizing the damage;
  - adoption of good practices and governance policy;
  - the prompt adoption of corrective measures; and
  - the proportionality between the severity of the breach and the intensity of the sanction.

Notably, Article 52 of the LGPD also contemplates the consideration of these factors in the particular case. The aggravating and mitigating factors applied in the Regulation to calculate a simple fine reference some, but not all, of the factors. In some instances, other sanctions, such as the blocking or deletion of personal data referenced below, do not reference these LGPD factors at all.

The ANPD should assess all of the Article 52 factors in each individual case to ensure that the sanction is proportionate to the risk of harm. We note that Article 28 of the Regulation allows for the substitution of sanctions where the established penalty is disproportionate to the harm caused, provided that other requirements, such as demonstrating the public interest protected, are met. We support this effort to incorporate an assessment of proportionality. However, to ensure a proper result in each individual case, the proportionality — along with all mitigating factors — should be assessed upon the initial assessment of the sanction.

We urge the ANPD to recognize all of the mitigating factors provided in Article 52 of the LGPD as part of case-specific fact-finding and imposition of appropriate sanctions.

III. Articulating Specific Criteria for Severe Non-Monetary Penalties

Effective data protection laws impose remedies that sufficiently deter law violations and, in some cases, include severe non-monetary penalties. For example, the LGPD identifies blocking of personal data , deletion of personal data, partial suspension of database operation, and suspension of processing activities as potential remedies for infractions. We recognize the need for the ANPD to have sufficient authority to address law violations, but we urge the ANPD to articulate specific criteria for conduct that warrants these serious sanctions.

- **Articulating Criteria for Application of Severe Non-Monetary Penalties.** Articles 22 through 25 of the Regulation authorize the temporary suspension of data treatment activities until the irregularity is addressed by the infringing party (referred to as blocking of personal data), deletion of personal data, partial suspension of database operation, and the suspension of processing activities, respectively. However, the Regulation does not articulate criteria for such severe non-monetary penalties. It notes only with respect to the suspensions (article 24) the factors that are considered for the duration of the suspension, but not the aspects considered for the underlying decision to impose the sanction. More specific criteria for applying such penalties are necessary to ensure the penalty is applied in a manner proportionate to the risk of harm, including the LGPD Article 52 criteria. The graduated sanctions recognize that some conduct warrants more lenient penalties, using warnings in some instances in lieu of financial penalties. Once a harsher sanction is imposed, there should be clear, articulable criteria that justify the higher-level penalty, and the sanctioned conduct should cause substantial harm. *We urge the ANPD to articulate more stringent criteria for these severe non-monetary penalties to ensure the penalty is narrowly tailored to address egregious conduct*.

* * *

BSA appreciates the ANPD's solicitation of feedback on the Regulation and would be pleased to serve as a resource for further consultation.

Sincerely,

BSA | The Software Alliance

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org