



December 6, 2023

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

Re: Regulation on the Performance of the Data Protection Officer

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 regulation on the performance of the Data Protection Officer (Regulation) under the Brazilian Personal Data Protection Law (LGPD).

BSA is the leading advocate for the global software industry. Our members are enterprise software and technology companies that create the business-to-business products and services to help their customers innovate and grow. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations.

We commend the ANPD for its efforts to recognize the important role of data protection officers (DPOs) under the LGPD. BSA supports data protection rules that are risk-based, technology neutral, and flexible. We recognize that organizations should develop policies and procedures to safeguard the personal data they process, including designating persons to coordinate programs implementing those safeguards and providing employee training and management;

¹ BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Palo Alto Networks, Prokon, Rubrik, 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.

regularly monitoring and assessing the implementation of those programs; and, where necessary, adjusting practices to address issues as they arise.

DPOs are now an established part of global data protection programs and can play a critical role in effectively implementing privacy safeguards across an organization.² However, companies vary in size, complexity, and volume of personal data processing. As a result, flexibility is needed to ensure that companies can establish a DPO role in a manner that best accommodates their business model.

We make several recommendations as you finalize the Regulation:

- We commend the ANPD for recognizing (in Article 13) that a single DPO may work on behalf of more than one processing agent, provided there is no conflict of interest. This provision is similar in kind to Article 37(2) of the GDPR, which permits a group of undertakings to appoint a single DPO so long as the DPO is easily accessible from each establishment. We encourage you to retain this approach in the final Regulation.
- We appreciate that the draft Regulation does not require a DPO be based in Brazil. Rather, the Regulation requires (in Article 11) that the DPO be able to communicate with the ANPD in Portuguese. We strongly recommend that the Regulation maintain this approach, to create flexibility for companies whose privacy expertise may be located outside of Brazil. Ensuring that companies may designate a DPO based on his or her expertise, rather than his or her geographical location, promotes global compliance efforts and ensures that companies can designate a DPO as part of centralized efforts to address privacy issues globally. In addition, we suggest the Regulation expressly state that the DPO may communicate with the ANPD via translator when necessary.
- We appreciate the Regulation's recognition (in Article 4) that it is a good governance practice for processors to appoint DPOs, including the Regulation's approach of positively taking into account such an appointment when assessing sanctions under the LGPD. We encourage the ANPD to retain this provision, which creates incentives for processors to appoint DPOs in line with the Regulation.
- We encourage the ANPD to clarify what it means (in Article 3) to appoint a DPO "by means of a formal act" and for the nomination to be published in an "official communication vehicle." The Regulation already requires (in Article 6) that the name and contact information of the DPO be published on a company's website. This ensures that data subjects and the ANPD can identify and contact the DPO. We recommend revising the Regulation to delete Article 3's additional means of nominating a DPO, which appear to be unnecessary. Alternatively, if these requirements are obtained, we encourage the ANPD to further specify how companies may satisfy the obligations.
- We recommend clarifying Article 20, which addresses the circumstances in which conflicts of interest are presumed. It is unclear from the draft text when such a conflict is presumed. One reading of the text is that a DPO is presumed to have a conflict if the

² See, e.g., GDPR arts. 37-39 (specifying circumstances under which it is necessary to appoint a data protection officer and specifying the officer's duties).

DPO also has competence to decide how a company processes personal data. We encourage the ANPD to clarify if this is the intended result.

* * *

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