



June 17, 2022

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

Re: ANPD Consultation on International Data Transfers

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 regulation of international data transfers 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. These technologies must transfer data across international borders – and across legal systems – to provide the global products and services that businesses demand. As a result, supporting the trusted and responsible transfer of data is a core issue for BSA members.

The need to transfer data internationally is not unique to technology companies – it is crucial for all companies that use technology, regardless of their size or industry sector. International data flows underpin today’s global economy and companies must transfer data every day to perform routine activities like processing payroll, working with suppliers, and serving customers worldwide. Companies need reliable and stable data transfer mechanisms that support responsible data flows.

We commend the ANPD for recognizing the importance of international data flows and for recognizing that data transfer mechanisms have become a key instrument for both protecting data subjects’ rights and for the development of the digital economy and international trade. We encourage you to prioritize transfer mechanisms that are based on high levels of data protection, trust, and confidence.

Our comments focus on three aspects of the consultation:

- ***Recognizing the benefits of international data transfers.***
- ***Promoting convergence and interoperability among contractual transfer mechanisms.***
- ***Suggesting practical options for implementing these requirements in practice.***

¹ BSA’s members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, 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.

Question 1: Obstacles to Transferring Data from Brazil.

Q: What are the current obstacles for companies to transfer data from Brazil to other countries? And from other countries to Brazil?

We welcome the consultation's recognition of the importance of cross-border data flows. Brazil will set important global precedents as it creates transfer mechanisms that support responsible data flows. International data transfers yield great societal and economic benefits, and rules that enable the transfer of data with adequate safeguards for privacy will help Brazil to realize those benefits. At a time of rising data protectionism across the world, Brazil should continue to promote strong privacy safeguards and international data flows as pillars of the data economy. Brazil should also be a strong voice against localization trends and other restrictions to international data flows that could limit Brazil's economic growth. This work is crucial in overcoming obstacles to transferring data across the globe.

Within Brazil, companies require a range of transfer mechanisms to support global data flows – and those mechanisms must be built on strong data protection safeguards. We support the ANPD's efforts to implement the LGPD's transfer obligations by ensuring that organizations have several practical options to use in transferring data across international borders, including adequacy determinations, standard contractual clauses, and other mechanisms. Different types of organizations and different business models require the use of different transfer mechanisms that are not interchangeable. In practice, larger companies will often rely on one or more data transfer mechanisms, using the tool most tailored to their business needs and to the specific data transfer(s) at hand. Other companies may principally rely only on one mechanism, such as adequacy determinations or standard contractual clauses. Creating a range of flexible transfer mechanisms that can be used differently in these different situations will help companies transfer data responsibly, consistent with Brazilian law.

One important step the ANPD can take before the new regulations are issued is to create certainty for international data transfers that are already occurring. Because the LGPD's provisions on international data transfers require implementation by the ANPD, there is currently uncertainty regarding the legal obligations for data transfers that occur before the forthcoming regulations are issued. We therefore recommend the ANPD issue guidance confirming that in the interim companies may continue to responsibly transfer data internationally based on global best practices, such as contractual provisions that ensure data remains protected regardless of where the data is transferred, when those best practices are consistent with the overall LGPD objectives. Under the current scenario – with few options available – organizations face more challenges to operate in a competitive international landscape. Developing regulations that operationalize the data transfer mechanisms under the LGPD is therefore critical to establishing legal certainty for organizations doing business in Brazil.

Question 2: Promoting Convergence and Interoperability

Q: What is the best way to promote convergence and interoperability between contractual instruments for international data transfers with instruments from other jurisdictions? And how can ANPD act in this regard?

Data transfer mechanisms cannot be viewed in isolation.

As countries worldwide develop and update their personal information protection laws and regulations it is critical that these legal frameworks are designed to effectively protect privacy in a manner that is internationally interoperable, flexible enough to account for rapid evolution in both technologies and business models, levels of risk, and that prioritizes high standards of data protection. This is particularly important in the context of international data transfers, where interoperable legal requirements support organizations' ability to comply with obligations across jurisdictions.

Of course, the context and perspective around privacy and personal data protection may appropriately vary among different countries based on cultural expectations, legal traditions, and other factors. At the

same time, governments should support the common recognition of international norms and practices around core substantive protections that underpin interoperable privacy frameworks. If countries instead adopt fragmented policies on core issues it raises the cost of business for all companies and can undermine personal data protection and consumer privacy.

Companies that provide services in more than one country must identify – and implement – additional privacy and data protection requirements imposed by each country in which they operate, keeping in mind how those obligations relate to regulations in other countries. Laws and regulations that promote convergence around internationally-recognized approaches to data transfers can help drive interoperable data transfer mechanisms, allowing companies to leverage these common approaches. In practice, a new transfer mechanism should be sufficiently similar – in structure and substantive protections – so that obligations under the new mechanism can be mapped onto obligations under the new mechanism. This ensures companies can understand how their obligations change across jurisdictions and allows them to identify shared requirements across legal frameworks. That approach creates a more efficient compliance process and drives investment in strong practices that companies can leverage in more than one jurisdiction.

There is an important role for policymakers in fostering such interoperable approaches to data transfers.

We strongly recommend the ANPD recognize that existing contractual transfer mechanisms may satisfy the LGPD's obligations, if they contain sufficiently similar substantive protections. Many global companies have already adopted contract-based transfer mechanisms that protect data as it is transferred between countries and regions. The ANPD may recognize that these existing contracts satisfy the LGPD if they contain sufficiently similar substantive protections as those required by the LGPD – without requiring companies to re-negotiate those contracts to adopt specific pre-approved language or formats. For example, if a company has adopted contracts that already incorporate the EU SCCs, that contract may contain sufficient data protection obligations to satisfy transfer requirements under the LGPD. We strongly encourage the ANPD to recognize that these existing contractual mechanisms may satisfy the substantive requirements of the LGPD and avoid requiring companies to adopt a new form or template that restates those protections. This approach drives harmonization by recognizing alignment between these existing mechanisms and the LGPD's requirements – and ensures that companies can leverage existing compliance practices and mechanisms in support of products, services, and customers in Brazil. In addition, participation in international certification systems can also advance convergence and interoperability.

It is paramount that the ANPD work to harmonize potential jurisdictional conflicts that may arise, to avoid leaving these issues to be dealt with by individual organizations.

Question 3: Widely Recognized Transfer Mechanisms.

Q: What are the most effective and the most used instruments to enable international data transfers by large and small companies or organizations?

As global companies, BSA members have adopted a range of contractual mechanisms to support responsible data transfers worldwide. Contractual mechanisms are particularly important for companies because they can support transfers to countries that have not received an adequacy determination and because they can be implemented without seeking prior approval from a regulator, unlike binding corporate rules. We therefore appreciate the ANPD prioritizing regulations that support contract-based transfer mechanisms.

BSA member companies have adopted contractual transfer mechanisms including the:

- European Union's Standard Contractual Clauses (EU SCCs);
- United Kingdom's International Data Transfer Agreements (UK IDTAs); and
- APEC Cross Border Privacy Rules System and the accompanying APEC Privacy Rules for Processors (APEC CBPRs and APEC PRPs)

Non-contractual mechanisms. Although the current consultation focuses on contractual transfer mechanisms, we also welcome the LGPD’s recognition of adequacy assessments and certifications, both of which support durable transfer mechanisms.

- *Adequacy.* Adequacy determinations are particularly important for small and medium-size enterprises that may lack the resources to adopt standardized contractual mechanisms. In making adequacy determinations, the ANPD can contribute to global convergence by recognizing other countries that create similar levels of data protection. Going forward, we encourage the ANPD to determine priority countries for adequacy decisions based on both the relevance for industry and on a country’s commitment to strong values of data protection.
- *Certifications.* In our view, certification schemes can contribute to a globally interoperable and market-driven system supporting data transfers. BSA recognizes that voluntary certification schemes can provide companies with flexible mechanisms for transferring data. We also want to emphasize that certification schemes are most useful for organizations if they are recognized and adopted by more than one jurisdiction – and therefore can permit companies using a single certification scheme to comply with obligations in multiple jurisdictions. We encourage the ANPD to prioritize these practical benefits in further considering certification schemes.

Question 4: Main Benefits and Impacts of International Data Transfers

Q: What are the main benefits and impacts of international data transfers, and what are the best alternatives for addressing them in each of the contractual instruments for data transfers included in the LGPD and in international practice?

We commend the ANPD for recognizing the benefits of international data transfers. We also appreciate your work to develop mechanisms that support the responsible flow of data across borders.

The ability to transfer data across international borders is critical to organizations of all sizes and across all industry sectors. Any company with employees, vendors, or offices in more than one country needs to send data internationally every day, including to:

- Manage global inventory through a centralized system, including routing products between countries;
- Analyze cybersecurity threats in different countries to identify common attackers;
- Manage human resources from a single headquarters; and
- Evaluate the performance of products and services from a single research hub.

For companies, transferring data across borders helps them be more efficient and effective at delivering the products and services their customers demand. Data transfers also underpin global products and services that support teleworking, virtual collaboration, online training, and online education, among many others. Having access to these global tools is particularly important for small- and medium-sized enterprises, which often leverage them to reach new markets and service new customers.²

Cross-border transfers are also integral to international supply chains, which must move information across borders to optimize sourcing, finance, logistics, risk mitigation, and responsiveness.³ The supply chain process for most products and services involves many phases, parties and countries – as well as potential disruptions based on weather, material availability, shortages, geopolitical threats, or emergent

² USAID Digital Strategy, 2020–2024, <https://www.usaid.gov/usaid-digital-strategy>, p. 37 (“Digital ecosystems have the potential to equip informal merchants, women entrepreneurs, smallholder farmers, and MSMEs engaged in cross-border trade with access to markets, information, and finance”).

³ Global Data Alliance, Cross-Border Data Transfers & Supply Chain Management, available at <https://www.globaldataalliance.org/downloads/03182021gdaprimersupplychain.pdf>.

health crises.⁴ In early 2020, 94 percent of Fortune 1000 companies reported supply chain disruptions from COVID-19,⁵ further highlighting the complex and integrated nature of supply chains and the role of data transfers in risk mitigation and response.

Data transfers aren't just important to companies individually – they also underpin today's global economy. Data transfers are estimated to contribute \$2.8 trillion to global GDP, a share that exceeds the global trade in goods and is expected to grow to \$11 trillion by 2025.⁶ Disruptions in cross-border data flows have broad reverberations that can lead to reduced potential GDP gains, reduced investments in local markets, job losses and consequently welfare losses, and adverse impact on local and national digital ecosystems – at a time when economic recovery is top of agenda for every government. Supporting international data flows can also help to develop a vibrant and thriving digital economy in Brazil.

To leverage the benefits that are brought about by responsible flow of data across borders, we recommend the ANPD promote convergence and interoperability of data transfer mechanisms, as discussed in our responses to Questions 2 and 3.

Question 6: Relationship of Adequacy Determinations and Contractual Transfer Mechanisms

Q: To what extent should the elements to be considered by ANPD in assessing the level of data protection of foreign countries or international bodies for adequacy purposes (article 34 of the LGPD) also be taken into account within the scope of the rules for contractual instruments?

We want to emphasize that adequacy determinations and contractual instruments are two separate mechanisms that support international data transfers. It is important to note that there is no hierarchy for the use of each mechanism provided for in Article 33 of the LGPD, including contractual instruments and adequacy. Parties are able to choose a mechanism that is suited to their transfers.

We encourage the ANPD not to apply the requirements for one of these mechanisms to the other mechanism. For example, companies that adopt contractual commitments for transferring data should not be required to assess the level of data protection of the foreign country to which data is to be transferred. That is because the contractual agreements themselves apply substantive protections to personal data regardless of where that data is transferred – making the contractual commitments appropriate for transfers to countries that have not received an adequacy determination. In addition, companies (and especially small and medium-sized businesses) are not equipped to perform the type of detailed and holistic assessment of a foreign country's laws and regulatory practices that an adequacy determination entails. Requiring such an assessment creates uncertainty as companies struggle with this task, which may have few benefits for consumers.

Question 7: Flexibility in SCCs

Q: Should the standard contractual clauses be rigid and with predefined content, or should their regulation allow certain flexibility concerning the text of the clauses, specifying the desired results and allowing changes as long as they do not conflict with the standard text made available?

⁴ According to the 2016 Global Climate Catastrophe Report, the supply chain industry faces an average of 260 major natural disasters annually

⁵ Erik Sherman, "94% of the Fortune 1000 are seeing coronavirus supply chain disruptions: report," Forbes, 21 February 2020. Available at <https://fortune.com/2020/02/21/fortune-1000-coronavirus-china-supply-chain-impact>.

⁶ OECD, *Measuring the Economic Value of Data and Cross-Border Data Flows*, 297 OECD Digital Economy Papers 24 (August 2020).

We strongly encourage the ANPD to prioritize a flexible approach to contractual transfer mechanisms.

As noted in our response to Question 2, we recommend the ANPD recognize that existing contractual transfer mechanisms may satisfy the LGPD's obligations, if they contain sufficiently similar substantive protections. This approach would specify the desired results – i.e., protecting data in line with the LGPD's requirements – rather than focusing on rigid requirements to adopt a certain format or a specific pre-approved language. A flexible approach is particularly important for ensuring that companies adopt the appropriate substantive obligations. Many companies have already entered into bespoke contracts that reflect existing legal obligations under other laws – and those commitments may also satisfy the substantive obligations under the LGPD. Companies should be able to rely on these bespoke provisions, provided they create sufficiently similar substantive protections to those required by the LGPD and do not conflict with any of the LGPD's requirements.

Question 8: Appropriate Format for SCCs

Q: What would be the most appropriate format for ANPD to make available models of standard contractual clauses for international data transfers? Are there any relevant tools that could be used to this end (e.g., decision tree, forms, checkboxes)? Are there any experiences on the theme that could serve as an example for ANPD?

We encourage the ANPD to prioritize flexibility in contractual transfer mechanisms. As explained in our responses to Questions 2 and 7, the appropriate format for standard contractual clauses should be flexible enough to recognize existing agreements that already meet substantive obligations of the LGPD

In addition, another interoperable approach the ANPD could consider to leveraging existing contractual mechanisms is to create a model addendum that can be added onto other contractual mechanisms, such as an addendum to the EU SCCs. The UK Information Commissioner's Office (UK ICO) recently adopted this approach in two new sets of model contractual clauses that came into force this year.⁷ First, the UK ICO adopted a 36-page standalone set of contract terms that companies could adopt to support transfers of data from the UK.⁸ Second, the UK ICO adopted a separate nine-page addendum, which companies can add to existing contracts that incorporate the EU SCCs; this allows companies to adopt the additional language in the addendum to support transfers of data from the UK.⁹ Adopting both a standalone set of SCCs and an addendum creates flexible options for companies transferring data from the UK, including for smaller businesses (which may not have other contractual mechanisms in place and thus may not make use of the addendum) and larger ones (which may already have existing contractual mechanisms that are readily modified by the addendum).

The creation of addendums – which recognize the substantive protections in the underlying contractual transfer mechanism and adopt a set of additional protections designed to satisfy the requirements of a second jurisdiction – is another interoperable approach to data transfers, designed to work across jurisdictions. We encourage the ANPD to further consider this model, which can help to ensure contractual mechanisms adopted by different jurisdictions can work together in practice to promote high data protection standards. At the same time, where existing contractual mechanisms may satisfy the LGPD's obligations, the use of addenda should not be required.

⁷ See UK ICO, International Data Transfer Agreement and Guidance, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/>.

⁸ See UK ICO, International Data Transfer Agreement, <https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf>.

⁹ See UK ICO, International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>.

Question 9: Modular Approaches to SCCs

Q: Is it necessary to have different rules depending on the type of processing agents (e.g., specific modules for controllers or processors) as data exporters or importers in international data transfers based on contractual clauses? If so, what would they be?

If the ANPD adopts new Brazilian SCCs, we encourage you to account for the range of different entities that transfer data and the range of different transfers between these entities. Any new contractual mechanism should support transfers between two controllers, from a controller to a processor, from a processor to a controller, or between processors. Data transfers take many shapes and forms and it is important that contractual transfer mechanisms can be used in the full range of transfer scenarios. For example, the EU recently updated its SCCs to adopt a modular approach that organizations can use to support these different types of transfers. Whether the ANPD adopts a modular approach or not, any new SCCs in Brazil should be flexible enough to be used in each of these scenarios.

Question 14: Verification of Specific Contractual Clauses.

Q: Are there any experiences with the verification and approval of specific contractual clauses and binding corporate rules that could serve as an example for ANPD?

Although this question refers to “verification” of specific contractual clauses and binding corporate rules, rather than verification of standard contractual clauses, we want to emphasize that the process of using contractual arrangements should not involve pre-approval by the ANPD. Rather, companies should be able to adopt contractual commitments that reflect the substantive protections required by the LGPD without asking the ANPD to approve each set of contractual terms in advance. This ensures that companies can readily adopt contractual transfer mechanisms, without creating a flood of approval requests that require attention by the ANPD and delay the adoption of mechanisms to safeguard transferred data. Instead, the ANPD should set forth specific requirements for contractual clauses and state that any contract meeting those requirements satisfies the LGPD’s obligations governing data transfers.

As for the approval of binding corporate rules (BCRs), the ANPD could consider accelerating the consideration of BCRs that have already been approved by other jurisdictions whose laws are analogous to the LGPD.

Question 17: Promoting Regulatory Compliance

Q: What are the best alternatives to promote regulatory compliance (including concerning the importer) regarding international data transfers?

We encourage the ANPD to promote regulatory compliance by issuing a range of guidance for industry about how transfer mechanisms are to be implemented under the LGPD. For example, the ANPD may create a website with resources for industry groups to learn more about the transfer mechanisms.¹⁰ The website may also be updated with specific guidance for particular industries or for small and medium-sized enterprises. We urge the ANPD to work with stakeholders throughout the process of adopting

¹⁰ For one example, see the UK ICO’s website on guidance to organizations, including data protection obligations after the UK’s exit from the European Union, available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/>

regulations on international data transfers, to identify areas where there is widespread agreement from stakeholders that additional regulatory guidance would be useful.

Question 19: Obligations Regarding Foreign Government Access

Q: What obligations should be assigned to the importer and exporter in case of access to data by foreign public authorities?

The consultation asks about obligations for the importer and exporter in the case of access to data by foreign public authorities. In the case of foreign government access, the appropriate obligation for a data importer is to notify the data exporter promptly if receives a legally binding request from a public authority or court in the third country to disclose the personal data transferred. At the same time, any such obligation must recognize that an importer may be prohibited by its national law from providing certain information to the exporter. In this circumstance, the importer's obligation should be to notify the exporter promptly after the expiration of any such prohibition, as permitted under applicable law.

In circumstances where there is no prohibition on notifying the exporter that a request was received by foreign public authorities, there may nonetheless be restrictions on the type of information that the importer may provide to the exporter about a request. We therefore recommend any obligations related to such notice avoid creating a rigid list of items to be contained in a notice, but instead recognize that any such notification is to include certain information, with a reasonable amount of detail, insofar as possible under applicable law. This creates more flexibility for data importers to provide notice to exporters, even if the importer may be prohibited from providing specific types of information.

Question 20: Transparency to Data Subjects

Q: What are the most appropriate mechanisms to provide data subjects with clear and relevant information about the possible transfer of their personal data outside of Brazil as well as to ensure the adequate protection of data subjects' rights in international data transfers? How should these instruments be implemented?

The consultation also asks about appropriate ways to provide data subjects with clear and relevant information about the transfer of their data outside of Brazil. We encourage the ANPD to focus on providing information to consumers that includes meaningful context – without requiring companies provide data subjects with long lists of data types or companies that may not advance the individual's understanding of how his or her data is handled. For example, we recommend against including any requirement to provide data subjects with the identities of all third parties to which personal data may be disclosed. Providing such information would result in a long list that could obscure relevant information for data subjects. In addition, providing such a list can be extremely difficult for companies to operationalize (given the amount of third parties that may be engaged to support a given service, and the need to switch among third parties during the course of providing that service). This would pull resources away from other activities that promote data protection and privacy.

In addition, we strongly encourage ANPD to refrain from creating strict requirements or mandating specific formats be followed for sharing information about data transfers. For example, companies should be allowed to share the necessary information with data subjects through websites.

As discussed in our response to Question 17, guidance for industry can also be helpful in creating tools that help companies implement policies in line with their obligations.

* * *

Thank you again for your focus on promoting interoperable mechanisms to support international data transfers. We welcome an opportunity to further engage with the ANPD on these important issues.

Sincerely,

Kate Goodloe
Senior Director, Policy