FINAL

CIPL Response to ANPD Request for Comments on the Regulation of International Data Transfers

Submitted 29 June 2022

International data transfer mechanisms have become a key instrument both for the adequate protection of data subjects' rights and for the development of the digital economy and international trade. Given the urgent need to regulate such mechanisms, ANPD plans to issue the regulation in stages. The first stage will have as scope the contractual instruments for international transfers of personal data, under article 33, II, (a), (b), and (c), of the LGPD, which are the standard contractual clauses, the specific contractual clauses, and the binding corporate rules.

To facilitate the understanding of the questions, consider "exporter" as the data processing agent[1] located in Brazil who will transfer the personal data to an importer situated in another jurisdiction, and "importer" as the processing agent located outside the Brazilian jurisdiction who will receive such data from the exporter.

ANPD welcomes contributions to any of the questions below. It is not mandatory to provide answers to all of the questions.

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

The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to comment on international data transfers and commends the ANPD on initiating the wide and inclusive consultation of key stakeholders on this critical topic.

Initially, CIPL notes that it would be helpful for ANPD to clarify the scope of what constitutes an international data transfer under Brazil's General Data Protection Law (LGPD) to which the various transfer mechanisms discussed below would apply. This would eliminate one preliminary obstacle to engaging in accountable data transfers. The European Data Protection Board (EDPB) addressed a similar issue in its Guidelines 05/2021, and we encourage ANPD to identify the criteria that would qualify a processing as an international transfer.

Specifically in response to the question, the principal obstacle for companies currently transferring personal data from Brazil is the lack of transfer mechanisms under LGPD arts. 33-36 duly regulated by ANPD.

If ANPD chooses to draft standard contractual clauses (SCCs) pursuant to LGPD art. 33(II)(a), CIPL encourages ANPD to develop simple, straightforward, high-level, outcome-based contractual clauses, ensuring that organizations have the flexibility to adapt provisions to their specific data processing

[1] *For the purposes of the Brazilian General Data Protection Law, the definition of processing agent refers to controllers or processors.*

[2] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 89 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

operations and transfer scenarios, including the flexibility to incorporate language already used in existing contractual instruments. Similar to the approaches taken by Australia, Hong Kong, New Zealand, and Singapore, ANPD could provide options for SMEs and startups with limited resources to create customizable clauses that would satisfy the LGPD's requirements. See, for example, the Model Contract Clauses Agreement Builder offered by New Zealand's Office of the Privacy Commissioner. For larger organizations with more robust resources, ANPD could list the type of protections and outcomes that need to be achieved and addressed in the contract under the LGPD and leave it to the parties to create the appropriate wording in their commercial contracts. Such a flexible approach to international data transfers would position ANPD as a global leader and could positively impact emerging privacy regulations in other countries as well.

ANPD could also take a further step by endorsing a high-level clause wherein the data recipient would simply guarantee compliance with the rights of the data subject and the obligations of the data protection regime under the LGPD. Such an outcome-based clause could be amended by the contracting parties with further specifications as needed under the circumstances.

Furthermore, ANPD could turn its focus to multilateral international certifications and mutual recognition measures, such as the Global Cross Border Privacy Rules (CBPR) system, discussed in response to Question 2.

Regardless of how ANPD decides to move forward, ANPD should provide a sufficient transition period for organizations to implement changes and satisfy the requirements of the new regulation. ANPD should also increase its outreach, engagement, and training with the impacted organizations to help drive understanding and compliance with the new rules. This is a new area of compliance for many Brazilian companies, and they will need some additional and specific direction through the process.

2) 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?

As explained in our answer to Question 1, CIPL encourages the development of simple, straightforward, high-level, outcome-based contractual clauses, ensuring that organizations have the flexibility to adapt provisions to their specific data processing operations and transfer scenarios, including the flexibility to incorporate language already used in existing contractual instruments. Outcome-based clauses ensure that the data recipient complies with the relevant data protection principles and obligations of the LGPD.

Also, ANPD should engage with the EU, UK, and other jurisdictions that have issued SCCs to explore ways to support mutual recognition of such instruments while ensuring (perhaps by way of an addendum, when needed) compliance with the LGPD's requirements.

CIPL notes that interoperability between contractual instruments is essential, both within Brazil and internationally, and should be enabled as much as possible. It ensures greater security and legal certainty for all existing and validated contractual instruments and helps organizations minimize administrative burdens and legal costs related to multiple sets of SCCs governing complex and multi-jurisdictional data flows.

In the same vein, ANPD should take into account privacy and data protection-related regulations already adopted by other regulators in Brazil (such as the Central Bank). We encourage ANPD to review such regulations and work with sectoral regulators to ensure consistency with the LGPD.

Moreover, ANPD should ensure that any contractual provisions relating to the international transfer of data are not so burdensome as to result in de facto data localization – a scenario where data may only be processed, accessed, and stored in Brazil. Such a framework would be highly onerous, harming both businesses and the Brazilian people.

CIPL further encourages ANPD to participate in the Global Cross Border Privacy Rules (CBPR) system in reliance on arts. 33(II)(d), 35 and 36 of the LGPD. The recently established Global CBPR Forum[3] is in the process of transitioning the current APEC CBPR into Global CBPR, which would enable non-APEC countries like Brazil to participate in the system. Participation in a global framework such as the CBPR has an added benefit of lessening the burden on resource-limited regulators like ANPD because front-line oversight and compliance are handled by third-party certification bodies, but ultimate enforceability would remain with ANPD and other global data protection authorities that participate in the system.

Similarly, we encourage ANPD to recognize the validity of certifications and other approval-based transfer mechanisms that organizations have received from other jurisdictions that offer the same level of protection as the LGPD, as they indicate that a robust regulatory review of processes and controls has taken place. This would enable organizations that already work with those transfer mechanisms to use them in Brazil as well, which would increase efficiency and reduce compliance costs.

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

Based on CIPL's 2016 and 2017 surveys with Avepoint on GDPR readiness, standard contractual clauses were the most popular transfer mechanism used, with about half of all respondents (49.6%) relying on model clauses for international transfers. We believe the findings are still relevant today. While use of the now-defunct Privacy Shield (for US-EU transfers) was the second most popular transfer mechanism at the time (averaging at 32.6%), many organizations are still maintaining certification in hopes of a new agreement between the US and EU. Roughly one-in-five (21.6%) relied on BCRs. See Organisational Readiness for the European Union General Data Protection Regulation.

a) Most organizations today use private contracts—in particular, standard contractual clauses (SCCs)—to legitimize the transfer of personal information across borders from jurisdictions that impose transfer restrictions, as there are so few other choices. Whether such contracts are "effective," however, is a matter of debate. Experts from industry and civil society have often commented that the use of lengthy, detailed SCCs is unsustainable in the long run, given the enormous and growing number of cross-border transfers to vendors, processors, sub-processors, third-party business partners, other data controllers, etc., and the fact that data transfers are dynamic, involve changing data sets, and are part of evolving business models. Indeed, SCCs are at times cumbersome and unworkable, especially for multiple transfers between multiple parties in multiple jurisdictions. To the extent ANPD is developing a framework for data transfers based on contracts, ANPD should consider SCCs that are outcome-based, flexible, and modular. See also our response to Question 1.

[3] For additional information, see the Global Cross-Border Privacy Rules Declaration, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

b) Certification and codes of conduct schemes may be the most effective data transfer instruments, since they are consistent and public, thereby enhancing accountability while avoiding excessive contractual paperwork. Many organizations were hoping to use certifications after the GDPR came into force, but this mechanism has not yet gained traction. Still, some organizations have obtained certification with the APEC CBPR, and with the launch of the Global CBPR Forum, there is an expectation that CBPR certifications will increase. For additional information on the Global CBPR Forum, see our response to Question 2.

c) Multinational companies use Binding Corporate Rules (BCRs) to enable intra-group data transfers (to and from internal controllers and processors) and transfers of controllers' data across an external processors' global organization (BCR processor). These companies see BCRs as a form of certification or seal to confirm trusted and protected data flows within the international group of companies, as well as a way to demonstrate compliance with local laws based on a single data privacy compliance program across multiple countries. BCRs require a significant investment of time and resources and therefore are currently limited to large, international organizations. For our views on BCRs, see our response to Question 5c.

d) Many organizations use (or would like to use more broadly) specific legal bases for particular types of transfers, such as when necessary for the execution of a contract or for compliance with a legal obligation. As provided in the LGPD, ANPD should clarify how organizations may use stand-alone legal bases for data transfers, including for routine and repeated transfers. Providing these legal bases for transfers would ensure that businesses relying on cross-border data flows for their products and services will not be blocked from the Brazilian market, as could happen if their ability to transfer data were jeopardized.

4) 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?

International data transfers drive today's global economy and growth. The ability to send (and receive) data from Brazil to other countries is critical to the success and security of Brazil's economy and society. The free flow of data allows organizations and individuals to access the best available technology and services at the best prices and safely engage in commerce, irrespective of where they are located. Today's digital economy and technologies demand that vast amounts of electronic data flow seamlessly across jurisdictions. The ability to use, share, and access information across borders enables research and development, fuels data-driven products and services, and promotes the exchange of ideas and information. It fosters innovation and competition by allowing new entrants access to data, which opens new markets and opportunities. It also benefits individuals, as it enables access to services and products across the globe and supports the growing reality of the Internet of Things.

International data transfers help organizations detect and prevent payment fraud and other crimes, and they also help them to conduct due diligence to comply with anti-money laundering (AML), counter-terrorist financing (CTF), anti-bribery and corruption (ABC), know-your-customer (KYC), and other rules. Data sharing across borders can also play a key role in countering discrimination and unconscious bias in development of AI technologies by providing access to larger, more representative and diverse data sets for the development of new artificial intelligence systems. Further, cross-border data flows can enhance data security and privacy protections. They ensure that companies of all sizes

can take advantage of decentralized data storage solutions and shared systems that are resilient to outages from malfunctions or natural disasters, as well as unauthorized access by third parties.

While the instruments for data transfers found in LGPD art. 33, II—namely, (a) specific contractual clauses for a given transfer, (b) standard contractual clauses, and (c) binding corporate rules (which are the three transfer mechanisms directly at issue in this consultation)—can all be useful to facilitate cross-border data flows in some contexts, they are not always well suited in their current forms for new technology trends (e.g., cloud platforms, artificial intelligence) and modern day data transfers that may include multiple parties, non-linear and fluid/dynamic data flows, and onward transfers between service providers and subcontractors.

To enable these data transfer mechanisms to achieve the outcome of facilitating and promoting free and trusted data flows, they should be made flexible and agile. For example, companies that have obtained approval for BCRs should be able to use them as a basis for transfers with another BCR-approved company, and not restricted to a single group of related entities for internal data transfers. This is a logical and progressive interpretation of BCRs, as both companies are deemed to have a high level of data protection within their groups for all data they process, including data received from other organizations. Equally, as mentioned above, contractual clauses must be flexible, modular, and outcome-based, to enable organizations of all sizes to use them with ease and without steep legal costs.

5) Which criteria and/or requirements should be considered in regulating each of the following international data transfer mechanisms and why?

a. standard contractual clauses;

Flexibility must be integrated in high-level, outcome-based clauses, ensuring that organizations have the ability to adapt provisions to their specific data processing operations and transfer scenarios, including the freedom to incorporate language already used in existing instruments. Outcome-based clauses ensure that the data recipient complies with the relevant data protection principles and obligations of the LGPD. A flexible instrument could provide a modular approach. It would also permit organizations to take risk factors into consideration, which would promote the efficient allocation of resources to implement additional safeguards to account for varying degrees of risk that might be associated with a particular transfer, keeping in mind that not all cross-border transfers are inherently risky.

b. specific contractual clauses; and

Initially, it would be helpful to clarify the distinction between standard contractual clauses and specific contractual clauses, which require prior authorization by ANPD before making a specific transfer. Because transfer-specific clauses with the attendant approval period could prolong negotiations and encumber commerce, CIPL encourages ANPD to streamline the process with a list of points to address or factors to be considered when drafting the clauses. ANPD could also develop a toolbox that provides guidance for organizations seeking the authorization of ANPD. But again, such clauses should afford a flexible, outcome-based approach.

c. binding corporate rules.

Binding corporate rules (BCRs) are currently data protection policies for the transfer of personal data within a group of undertakings or enterprises. Because BCRs require a significant investment of time and resources, BCRs are commonly an option only for large, international organizations. To facilitate

their wider use, BCRs need to be made scalable and configurable to the needs of organizations of all sizes and corporate structures. Moreover, their use should be explored beyond the confines of intra-corporate transfers (as discussed more fully below in response to Questions 10 and 11). Indeed, ANPD can play an important role in expanding the reach and accessibility of BCRs to small and medium enterprises (SMEs).

CIPL also encourages ANPD to consider the following suggestions pursuant to art. 33(II)(c), art. 35, and art. 36 of the LGPD:

- Endorse BCRs authorized by the EU, the UK, and other jurisdictions based on art. 35 of the LGPD. Upon accession to those BCRs, Brazilian entities within the corporate family would assume all the rights and obligations according to the existing BCRs. This can significantly facilitate compliance with applicable rules for companies active in the EU, the UK, and Brazil.
- Engage with regulators in the EU and UK (and other jurisdictions with BCRs) to support mutual recognition of BCRs developed by the ANPD.
- Recognize existing BCRs in force and approved in other jurisdictions that offer the same level of protection as the LGPD.
- Avoid creating new specific requirements just for Brazil so that BCRs approved by a company in another jurisdiction do not work in Brazil, or even worse, create conflicts between different sets of BCRs.
- Define clear and workable criteria for reviewing and approving BCRs, perhaps creating an expedited process for approval/adoption/recognition of BCRs already approved in other jurisdictions that offer the same level of protection as the LGPD.
- Create a proportionate, flexible, and interoperable approach to BCRs that enables the efficient movement of data across borders between different corporate groups, groups of undertakings, or enterprises engaged in a joint economic activity such as franchises, joint ventures, or professional partnerships.
- Develop a user-friendly and streamlined application framework and approval process.
- Consider accrediting third-party organizations to play a due diligence role in the BCR approval process to assist ANPD and help streamline its BCR approval operations.
- Create a toolbox, templates, and guidance inspired by the documents issued by the Article 29 Data Protection Working Party (WP263, WP264, WP265, WP256, WP257).

6) 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?

ANPD should not conflate adequacy determinations with SCCs and other contractual instruments. Organizations are facing major difficulties following the decision of the Court of Justice of the European Union in *Schrems II*, which requires companies to conduct transfer impact assessments (or transfer risk assessments) to evaluate whether their envisioned transfer to the importing country is afforded an essentially equivalent standard of data protection to that of the EU, when taking into consideration available appropriate safeguards and potential supplemental measures. If Brazil were to follow a similar approach, it would impose a requirement on organizations that is not and should not be within their remit (i.e., to examine the data protection regime of every country to which they transfer personal information). Requiring individual organizations to comprehensively assess the privacy and data protection regimes of individual countries and to determine "transfer risks" on the basis of such assessments is unduly burdensome, ineffective, unreliable, inefficient, and oftentimes

impossible (especially for SMEs and start-ups with limited resources). Moreover, requiring organizations to conduct assessments would undermine the role of ANPD, as the LGPD is clear in art. 33(1) and art. 34 that adequacy assessments are within the remit of the ANPD. Organizations should simply be responsible for ensuring (through compliance with LGPD art. 33) that the company to which they transfer data remains accountable under Brazilian standards for the data it receives from Brazil.

Similarly, ANPD must be cognizant of the different roles that SCCs and adequacy determinations play in the global transfer arena. SCCs are typically used in instances where a country does not have an adequacy determination from the exporting country. As such, it would not make sense to include an assessment of country-level adequacy as part of the requirements for transfers via contractual instruments, as contracts are business-to-business tools, and do not address broader country-level adequacy issues. In CIPL's view, any assessment of a particular country's use of data for national security and intelligence purposes (and any related assessment of a country's means of redress for alleged violations thereof) is beyond the capabilities and competencies of most private organizations.

7) ***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?***

As stated above, SCCs must be designed in a way that affords organizations appropriate flexibility to adapt them to their specific processing activities and transfer scenarios, including the freedom to incorporate language already used in existing instruments. Indeed, the rigidity associated with the EU standard contractual clauses has been a challenge for organizations for many years. CIPL (along with many other industry bodies, trade associations, and organizations) advocated for a more flexible approach during the EU Commission's update of the pre-GDPR SCCs. (See CIPL White Paper on Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR). Thus, while the uniformity of standard clauses across industries has certain benefits, SCCs should nevertheless permit sufficient flexibility to account for differences in organizational structures or unique processing ecosystems.

ANPD should design clauses that are flexible from the start. For example, the clauses should not dictate the number of parties to the contract or the nature of the processing operations that can be covered, and organizations should be able to modify and adapt some of the language to ensure that the contractual clauses can work in practice for the transfer at hand.

8) ***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?***

As mentioned above, CIPL encourages the development of outcome-based clauses, ensuring that organizations have the flexibility to adapt provisions to their specific data processing operations and transfer scenarios, including the flexibility to incorporate language already used in existing instruments. Outcome-based clauses ensure that the data recipient complies with the relevant data protection principles and obligations of the LGPD. These clauses can set out, for example, the outcomes and objectives to be achieved, such as data security during transmission and processing by the data importer, assistance with the data subject's rights by the data importer, a prohibition on

further processing for unrelated purposes by the data importer, etc. By specifying topics and outcomes, companies can be flexible in how they implement the actual requirements in their contracts. A flexible instrument could provide a modular approach. It would also permit organizations to take risk factors into consideration, which would promote the efficient allocation of resources to account for varying degrees of risk.

A decision tree to address desired outcomes would be helpful, as would a checklist to help determine which clauses would be applicable to a specific transfer. Given that international data transfers apply to a very broad spectrum of transfers, a modular approach that reflects requirements based on risk would be helpful. Moreover, a questionnaire, such as the Model Contract Clauses Agreement Builder offered by New Zealand's Office of the Privacy Commissioner, should be considered as an option for creating more customizable clauses. Whatever tools or resources ANPD creates should be viewed only as guides and should not be rigid or mandatory.

9) 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?

Because controllers and processors have different obligations, it is important for contractual clauses to be versatile or adaptable enough to reflect the actual roles and responsibilities of the parties. And the clauses must be able to be easily incorporated into any data processing agreements and related documents. Because a data recipient can sometimes act as both a controller and a processor, contractual clauses should never be one-size-fits-all; rather, they should be able to be applied flexibly depending on the context of the transfer.

In addition, controllers must ensure that their operators and sub-operators (processors and sub-processors) respect and protect the personal data entrusted to them, complying with all of the criteria and standards of the LGPD. In this regard, operators must comply with the controller's instructions and always ensure the security of personal data present in their systems. These requirements are already present in the LGPD – any contractual clauses regarding international transfers must ensure that these obligations do not end at the borders of Brazil. Such an approach is consistent with the LGPD's accountability standards, which apply regardless of where the data will be transferred.

10) Are there requirements that need to be different for Binding Corporate Rules from those usually required for Standard Contractual Clauses? If so, what would they be?

Yes. SCCs (as currently configured) impose on data importers obligations specific to their role as data importers and specific to the personal data at issue in the transfer. BCRs, by contrast, encompass a binding and enforceable code of conduct addressing all transfers of personal data within a group of undertakings or group of enterprises engaged in joint economic activity. BCRs include requirements relating to a comprehensive privacy program and compliance ecosystem, such as governance mechanisms, DPOs, policies and procedures, training and communication, and audits and assessments. Thus, BCRs are, in essence, an accountability mechanism, which supports compliance with local law, as well as enabling adequate protection for data transferred across borders. Because BCRs align closely with a company-level "adequacy" model, CIPL would encourage the use of BCRs beyond the context of intra-corporate transfers to enable transfers also between different corporate groups that have BCRs.

BCRs require a significant investment of time and resources and therefore are currently limited to large, international organizations. To enable SMEs to reap the benefits of BCRs without the attendant time and expense, ANPD may wish to consider an SME-friendly version of BCRs—provisionally called "Intra-Group Data Transfer Agreements"—as an alternative. These transfer agreements are a hybrid between contracts and BCRs and could potentially be an option for SMEs. They could also provide an opportunity for ANPD to work toward the adoption of norms that would not require as great an investment as do traditional BCRs, but would still provide "company-level" assurance for data transfers.

11) How should a corporate group be defined for the purpose of application of Binding Corporate Rules?

CIPL encourages ANPD to consider the factors mentioned by the Article 29 Data Protection Working Party in the EU (the predecessor of the European Data Protection Board (EDPB)) in the following guidance:

> [t]he notion of "corporate group" may vary from one country to another and may correspond to very different business realities: from closely-knit, highly hierarchically structured multinational companies to groups of loose conglomerates; from groups of companies sharing very similar economical activities and therefore processing operations to broad partnerships of companies with very different economical activities and different processing operations. Obviously, these differences in structure and activity impacts upon the applicability, design and scope of the binding corporate rules, and corporate groups must bear this in mind when submitting their proposals.[4]

However ANPD chooses to define "corporate group," it is important that the group complies with the BCRs.

Moreover, CIPL suggests that BCRs enable data transfers not only within corporate groups (however defined), but also between entities of different corporate groups that have BCRs, where the BCRs are based on the same underlying law or standard. That would significantly improve the usefulness of BCRs. Moreover, ANPD should consider options that would introduce more flexibility for SMEs, such as the Intra-Group Data Transfer Agreements discussed in response to Question 10.

12) What is the minimum information (level of detail) on personal data needed to allow proper compliance analysis by ANPD of the international transfers of data carried out by contractual instruments, in order to minimize negative impacts on business activities and preserve a high degree of protection for the data subject?

To refrain from imposing an excessive burden on contracting parties and to ensure agility in the preparation and negotiation of contractual instruments, the description of operations included in the relevant instruments must contain only the basic elements for the examination and understanding of the data flow. Thus, while international transfers should be assessed in the context of an overall accountability principle, data maps and data flows fluctuate over time and therefore should not be

[4] See: Article 29 Data Protection Working Party, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Draft Working Document on Binding Corporate Rules for International Data Transfers (on the basis of the discussions of the Sub (europa.eu).

used as a basis for demonstrating compliance. Companies should not be required to complete appendices or annexes as is done in the EU. See also our responses to Questions 4 and 5.

It should be noted that the LGPD, in art. 35, §2, grants the ANPD authority, on a case-by-case basis, to request additional information or carry out verification procedures when analyzing contractual instruments. This, we believe, is a clear indication from the legislature that ANPD, in the first instance, should draft practical contractual instruments, reserving the need to request additional information only for specific situations.

13) What are the risks and benefits of allowing transfers between different economic groups whose binding corporate rules have been approved by ANPD?

The benefits of allowing transfers between unaffiliated companies based on BCRs are significant, as it would dramatically increase the value and application of BCRs. If one BCR-approved organization is permitted to transfer data to and from another BCR-approved organization subject to the terms by which both organizations are already bound, both organizations would reap huge benefits from the assurance that each organization's comprehensive privacy program and compliance infrastructure already pass muster, and individuals would be able to share that assurance as well. In this scenario, BCRs would essentially function as a certification of appropriate privacy protections. CIPL foresees no risks from such an arrangement, rather, only benefits and incentives for more organizations to adopt a holistic and high level of protection envisaged by BCRs. We believe there will be a lot of interest in the market in this type of instrument. Evidence shows that companies are keen to be able to demonstrate that they are a trusted data steward and business partner no matter where they operate and where data comes from or goes to (both to consumers and in B2B relationships).

14) 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?

In view of the experience in Europe, ANPD should be aware of the resourcing constraints resulting from the current model of adoption/refresh of BCRs. The adoption of BCRs in the EU is accurately perceived as a lengthy and burdensome process that requires a significant amount of resources and executive support. Many regulators are experiencing difficulties in resourcing BCR reviews and addressing back-logs of BCR applications, which should also be considered. ANPD should draw on this experience and consider a model whereby BCRs and similar instruments for international data transfers, like "intra group data transfer agreements," can be approved by third-party approval organizations without intensive involvement of the data protection authority. See also our response to Question 10. Such a system would still enable ANPD to hold organizations accountable for their BCR promise and "certification", as ANPD would be able to demand demonstration of compliance or investigate in case of a suspected breach by a company with BCRs.

Moreover, given that the approval of BCRs implies a considerable use of resources on the part of ANPD, we believe that a more accessible transfer mechanism could be participation in the Global CBPR. The use of accountability agents could enable more companies to accede to a solid transfer mechanism and lessen the resource pressure on ANPD. Furthermore, as mentioned in our response to Question 5c, ANPD should consider recognizing BCRs already approved by the EU, UK, and other countries.

As for specific contractual clauses, see our response to Question 5b.

15) What are the data subject's rights in case of changes in the original configuration of the transfer? In which situations is it essential to communicate directly with the data subjects or to enable some type of intervention by them?

Please refer to our response to Question 16. To the extent this question is asking about the role of data subject rights (DSRs) in the context of international data transfers, it is important to note that DSRs are not absolute and that transparency does not mandate control by individuals over the purpose of the transfer and the location of the data. Approval of data subjects should not be required, nor should they be allowed to intervene in contractual arrangements between the data exporter and importer or have a say on the decision of the mechanism used to transfer data, if the mechanism used is in compliance with the LGPD. Data subjects need to be informed and allowed intervention only if there is a change to a transfer that was done based on their consent. They should also be able to seek assistance with the original controller/data exporter in case of any data protection breaches resulting from a data transfer to another country.

16) What are the best alternatives for resolving conflicts between processing agents and/or between those agents and data subjects involving contractual instruments for international data transfers? Could bilateral, multilateral or international cooperation between data protection authorities assist in conflict resolution? If so, how?

Chapter IX of the LGPD describes the powers granted to ANPD. Among these powers, there is no mention of arbitration or mediation prerogatives. Therefore, it is important that ANPD remains within the scope of its mandate and avoids intervening in contractual disputes. The parties should be primarily responsible for solving any contractual disputes as well as any issues with the data subject.

However, we can foresee a situation where a cooperation between ANPD and the DPA of the importing country may be helpful and yield results, especially where the data exporter is not able to effectuate any change or solve the issue for the data subject and the problem or breach is on the part of the data importer. Of course, a data subject's first recourse is with the data exporter, but in the absence of an amicable resolution, a complaint to ANPD would be in order, and, if necessary, ANPD may need to reach out to the DPA of the importing country for clarification and potential resolution of outstanding issues. With respect to contractual instruments, conflicts around international data transfers should be solved with the means provided by the relevant contractual law.

The Global CBPR system effectively addresses violations of data privacy laws in the context of cross-border transfers, as it incorporates participation from data protection authorities in the Cross-border Privacy Enforcement Arrangement (CPEA). The CPEA provides mechanisms to promote effective cross-border cooperation between authorities in the enforcement of data protection law, including through referrals of matters and through parallel or joint investigations or enforcement actions. In addition, companies participating in the CBPR must use dispute settlement mechanisms provided to individuals by the accountability agents. These are effective and accessible tools to resolve conflicts.

In addition to the CBPR Forum, we encourage ANPD to promote interoperability between data protection and privacy regimes and facilitating international flows of personal data via the Ibero-American Data Protection Network and the Global Privacy Assembly.

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

Please refer to our responses to Questions 3, 4, and 10. Additionally, we commend ANPD for providing this opportunity to comment on international data transfers, and we encourage ANPD to continue to dialogue with organizations and individuals as it develops guidance and clarifications regarding compliance with the LGPD.

18) What are the best alternatives to resolve practical issues related to the accountability of stakeholders who transfer data overseas, especially in cases where onward transfers to other jurisdictions occur or when data is processed by other data processing agents in the same jurisdiction?

Mandatory adoption of the same or substantially similar contractual clauses in all onward data transfers is likely the best alternative to resolve practical issues related to the accountability of stakeholders. In cases where onward transfers to other jurisdictions occur or when data is processed by other data processing agents in the same jurisdiction, the parties involved and especially the data importer should require that substantially similar protections are adopted for onward transfers.

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

Practices with respect to government access should align with internationally recognized frameworks, and any issues should be resolved at the political level between governments through fora such as the OECD, which has developed a working group on trusted government access. Organizations should have policies and procedures in place to screen incoming requests and to respond in an appropriate manner. There should be no general notice requirements relating to appropriate and legitimate governmental access requests either to the ANPD or data subjects.

Requiring individual organizations to comprehensively assess the privacy and data protection regimes of individual countries, sectors, and industries and to determine "transfer risks" on the basis of such assessments is unduly burdensome, ineffective, unreliable, inefficient, and oftentimes impossible (especially for SMEs and start-ups with limited resources). In CIPL's view, any assessment of a particular country's use of data for national security and intelligence purposes (and any related assessment of a country's means of redress for alleged violations thereof) is beyond the capabilities and competencies of most private organizations. Indeed, as discussed in response to Question 6, under art. 34 of the LGPD, country adequacy determinations are within the remit of ANPD. What would be appropriate, however, is to require importing organizations to have internal procedures in place to respond to government access requests in a manner that ensures due process, data minimization, and proportionality.

When requesting data from U.S.-based providers, countries should utilize existing legal channels, such as requesting data production through the U.S. Mutual Legal Assistance Treaty (MLAT) process and through ratification of the Budapest Convention and the Second Additional Protocol to avoid conflicts of law. We also support new models for bilateral agreements between rights-respecting governments that improve cross-border access to digital evidence, like the CLOUD Act.

If a sovereign State requests disclosure of data that is under the control of an entity under the jurisdiction of another sovereign State, the MLAT process should be used to reconcile Brazilian

sovereignty with the sovereignty of the foreign State. The Brazilian Federal Constitution, in art. 4, items VII and IX, establishes a duty of cooperating with other governments for the progress of humanity, as well as the peaceful resolution of conflicts. Similarly, the Code of Civil Procedure has dedicated a specific chapter to the need for this kind of international cooperation. The LGPD also highlights international cooperation in art. 33, III and VI.

20) 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 goal should be that all data is used and transferred within a compliant and accountable legal framework—such as SCCs, BCRs, or Global CBPR—so that individuals need not worry about whether their data is in Brazil or elsewhere because it will always be protected at the appropriate level. While individuals should be informed that their data will be subject to appropriate protections and safeguards regardless of where it travels, ANPD should not create strict requirements or mandate specific formats on how to convey such information. Instead, ANPD should develop guidelines that support transparency with flexibility.