20 CIPL

CIPL AT 20 — SHAPING DATA POLICY FOR TOMORROW

HUNTON ANDREWS KURTH

ANPD Autoridade Nacional de Proteção de Dados

MODEL FOR CONTRIBUTIONS CONCERNING THE PRELIMINARY INPUTS Nº 1/2021

NAME OF INSTITUTION: Centre for Information Policy Leadership (CIPL)

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUCTION

The following questions seek to guide the taking of preliminary inputs from the new regulation applicable to micro and small businesses, as well as incremental or disruptive business initiatives that declare themselves to be start-ups or innovation companies and individuals that process personal data for economic purposes, as provided in art. 55-J, XVIII, of the LGPD and item 3 of the ANPD Work Plan 2021-2022.

Below are (i) general questions, concerning identifying the main data protection regulatory challenges for SMEs including through mapping international experiences, (ii) specific issues, such as the definition of micro and small businesses that are most suitable for the sectoral regulation of data protection and privacy, the impact of LGPD rules on SMEs (maintenance of the records of processing, operationalisation of a data processing impact assessment, compliant data processing, designation of the data protection officer, right to data portability, data security measures, data protection management and compliance programs and good practice), and (iii) questions concerning regulatory alternatives to encourage and promote innovation by SMEs.

Contributors can insert other relevant topics in the table below.

ABOUT CIPL

The Centre for Information Policy Leadership (CIPL) welcomes the opportunity to respond to the first public consultation organised by the Autoridade Nacional de Proteção de Dados (ANPD) and would like to compliment ANPD for seeking cooperation with, and inputs from, multiple stakeholders.

CIPL is a global data privacy and cybersecurity think tank based in Washington DC, London and Brussels, founded in 2001 by the law firm of Hunton Andrews Kurth LLP. 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. We work with senior leaders and privacy experts of 75+ leading global organisations who provide us real inputs into their data privacy practice and decision-making. See more about CIPL at https://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.

CONTRIBUTIONS **IMPORTANT:** The inputs below must be justified. Contributors must add the appropriate references (links) to any international norms mentioned.	
TOPICS/QUESTIONS	**CONTRIBUTION/INSTITUTION**
What are the regulatory challenges/problems concerning this topic?	The new Brazilian data protection law (*Lei Geral de Proteção de Dados* – LGPD) provides that ANPD must draft specific rules concerning SMEs' compliance with this law (Article 55-J, XVIII). CIPL understands that many organisations and industry associations have been advocating for SMEs be exempted from a series of LGPD provisions. While exemptions may be appropriate in some cases, the **Autoridade Nacional de Proteção de Dados (ANPD) must (i) be flexible while being reasonable and following the LGPD's risk-based approach nature when drafting further rules that may exempt SMEs from LGPD provisions, and (ii) focus on the best outcomes for individuals and society taking into account the various challenges and risks that relate to this topic, outlined below**: • Due to the LGPD being the first comprehensive data protection law in Brazil, there is a general lack of awareness and overall low level of maturity on this topic, including among SMEs; • The LGPD went into effect in the middle of the COVID-19 pandemic. While COVID-19 represented opportunities for some industry sectors and larger organisations, many SMEs have been heavily impacted and had to shift their already scarce resources to surviving the crisis rather than complying with the new data protection rules. There are concerns that many will be unable to resume their businesses after the crisis; • The lack of clarity concerning the scope of applicability of the LGPD to SMEs leads to SMEs either (i) incurring unnecessary compliance costs that may not be proportionate to the nature of the risks for the data subjects, or (ii) not being able to effectively comply with the LGPD rules overall;

	• Non-compliance with the LGPD, in particular among SMEs, risks rendering the LGPD ineffective and consequently decreasing the level of protection to Brazilians. This may result in a knock-on effect in which larger private organisations, as well as public sector organisations, may not take the LGPD rules seriously, which will ultimately hinder the development of Brazil's digital economy and innovation, and prevent the development of a data protection culture in Brazil. A general lack of compliance and LGPD effectiveness may negatively impact future decisions of adequacy or bilateral agreements for the purposes of international data transfers between Brazil and other countries; • Lack of compliance of SMEs with the LGPD (and in particular those SMEs that have a data-driven business model) risks creating a compliance gap in the digital supply chain that may *de facto* exclude them from further business opportunities and development. This could be the case if SMEs fail to comply with the LGPD rules or if they are granted compliance exemptions. A CIPL member who is an international organisation have reported that in some cases they currently decide to not engage with Brazilian SMEs given that SMEs are unable to fulfil their due diligence requirements concerning information security that are required by non-Brazilian laws and standards. Moreover, some CIPL members have reported that they might consider not engaging with Brazilian SMEs as vendors/processors/business partners if further exemptions that may be provided by the ANPD lead to SMEs not effectively protecting personal data as appropriate to the risks of their data processing activities as this may impact the overall compliance of these CIPL members; • Therefore, the ANPD's main challenge is two-fold: to (i) provide flexible and scalable rules to SMEs that enable compliance with the LGPD, encourage them to become accountable, and facilitate their effective functioning in a data-driven Brazilian economy post COVID-19, and (ii) avoid excessive exemptions to compliance and enforcement rules that lead to SMEs not complying with other applicable LGPD rules as appropriate to the risk of their data processing activities and not fearing enforcement by the ANPD. See for reference the following CIPL papers: • Looking Beyond COVID-19: Future Impacts on Data Protection and the Role of the Data Protection Authorities (2 June 2020) • The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society (23 July 2018) – for more information concerning the impact of accountability on contractual provisions and negotiations within supply chains

What are your suggestions for addressing these problems?	There are a series of measures that the ANPD can take to address the challenges and risks outlined above in a risk-based and outcomes-based manner: • **Providing guidance to SMEs** – the ANPD should prioritise providing guidance to SMEs to clarify the many applicable LGPD provisions and help them understand the importance of protecting personal data and becoming accountable. ○ Guidance should focus not only on (i) the most important LGPD provisions (e.g. requirements concerning data privacy notices and transparency, appointing a Data Protection Officer (DPO), undertaking a Data Protection Impact Assessment (DPIA), maintaining records of processing activities, etc.) but also on (ii) data protection topics that are key enablers of SMEs' use of personal data for innovation (e.g. data sharing, legitimate interests, pseudonymisation and anonymisation, algorithmic training relying on personal data, international data transfers, etc.); ○ The ANPD should work with industry associations to identify what are the most pressing topics for SMEs; ○ Any guidance provided by the ANPD to SMEs should be written in simple and plain language (as opposed to legalistic language), be concise, and pragmatic (i.e. address the practical operational needs of SMEs); ○ There are many ways that the ANPD could provide such guidance, such as through formal guidelines documents, a page on the ANPD website dedicated to SMEs gathering relevant resources, FAQs, one-pagers, case studies, examples of best practices, do's and don'ts, showing what good and bad look like, etc. (see our response to the questions "What are the international experiences regarding this topic?" and " How has the EU addressed compliance of SMEs with the General Data Protection Regulation (GDPR)?" for examples of what other data protection regulators are doing to provide guidance to SMEs); • **Developing and promoting accountability and compliance tools and templates for SMEs** – including templates (such as for records of processing, DPIAs, legitimate interest assessments), automated questionnaires, checklists (such as for the key components of a data governance programme), self-assessment tools and others. The ANPD should, however, make clear that such tools and templates are recommendations as opposed to mandatory, and that SMEs as well as larger organisations should be free to use any other tools and templates they consider to be most appropriate for reaching the data protection outcomes sought;

	• **Encouraging the development of industry codes of conduct** – see response to question "What regulatory mechanisms could be used to promote and incentivise innovation by SMEs?" below; • **Enabling the development of certifications, seals and marks** – as they have the potential to play a significant role in enabling organisations, in particular SMEs, to achieve and demonstrate organisational accountability, and therefore place themselves in a better competitive position; • **Encouraging sharing of good practices in data protection, data management and data hygiene among Brazilian professional organisations** – through industry initiatives such as roundtables, benchmarking, creation of DPO networks, publication of templates and methodologies used by industry, recognition of accountability frameworks such as the CIPL Accountability Framework (see figure below) for the development of data governance programs, raising awareness of the benefits of accountability (see Cisco's 2021 Data Privacy Benchmark Study). In particular, the ANPD should encourage larger, more mature organisations to share their best practices and tools to SMEs (e.g. larger technology companies supporting third party developers' LGPD compliance through sharing of information and good practice), as this would help enhance compliance and accountability across the entire data ecosystem. Larger and more mature organisations have a key role to play in pushing accountability down through the supplier/vendor chain; • **Driving SME-focused education and awareness programs**; • **Providing opportunities for SMEs to engage with the ANPD and share their compliance experience** – for instance through roundtables, sandboxes (see our response to the question "What regulatory mechanisms could be used to promote and incentivise innovation by SMEs?" below), questionnaires, surveys, etc.; • **Taking organisational accountability efforts into account when enforcing the LGPD rules against SMEs and being transparent about this in connection with relevant enforcement criteria** – this will encourage SMEs as well as larger organisations to implement the principle of accountability, ultimately leading to enhancement of trust in the data ecosystem; • **Enabling international transfers of personal data to enable Brazilian SMEs participate in the global digital economy** – through:

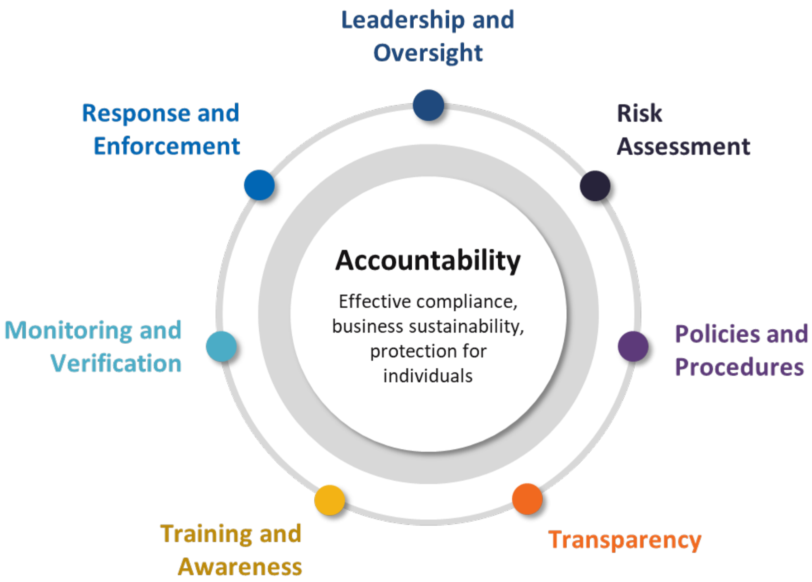
    - The development of data transfers mechanisms and guidance concerning these mechanisms (e.g. standard contractual clauses, binding corporate rules, codes of conduct, certifications, seals and marks);
    - Encouraging Brazil to join regulatory data transfers schemes such as the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) System when this opens to non-APEC countries;
    - Recognising international certifications such as ISO certifications, as well as binding corporate rules obtained under other data protection regimes as valid data transfers mechanisms; and
    - Encouraging Brazil to negotiate bilateral data transfers agreements;

- **Working with public authorities of other regulated areas as well as industry associations to identify cross-sectoral initiatives to support SMEs' LGPD compliance** – SMEs are subject to overlapping rules in Brazil and would also benefit from awareness-raising activities and other initiatives (e.g. cross-sectoral sandboxes and roundtables, joint-guidance) that would help them navigate complex legal scenarios when processing personal data; and
- **In particular, when providing guidance and tools to SMEs, the ANPD should prioritise promoting the principle of accountability as enabler of effective data protection and responsible uses of personal data, and as a baseline for LGPD compliance** – the accountability principle is emerging in data protection laws and in other compliance areas such as competition and compliance laws, anti-corruption laws, and others. This would enable SMEs to leverage the compliance efforts done in the data protection field for other compliance areas and vice-versa.

Accountability is globally recognised as a key building block for effective data privacy regulation. Ever since the inclusion of the accountability principle in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, accountability has been recognised in many data protection laws and frameworks as a core principle. It means that organisations:

- Take steps such as implementing a comprehensive data governance and compliance programme to translate data privacy legal requirements into risk-based, concrete, verifiable and enforceable actions and controls relating to the processing of personal data which are reviewed and adapted over time; and
- Are able to demonstrate the existence and effectiveness of data governance programmes internally (e.g. to the board and senior management) and externally (e.g. to privacy enforcement authorities, individuals, business partners and shareholders).

	CIPL has worked extensively on accountability and has been advocating for the uptake and implementation of accountability by organisations of all sizes and regulators around the world. In 2020, CIPL completed an accountability mapping project where we analysed and mapped real accountability measures undertaken by 17 organisations of various industry sectors, sizes and regions, including two SMEs and a university. This led to a number of trends identified in relation to accountability, including that **accountability is a scalable and sector-agnostic concept. That is, organisations of all types, sizes, sectors (including the public sector), geographical footprints and varying corporate cultures can develop and implement accountable data governance programmes, even SMEs**. The programme, the specific activities (policies, procedures, controls and tools) and the human and financial resources may be different depending on the specific context, risks, goals and size of each organisation. In particular, while smaller organisations can and do take steps to be accountable, they calibrate measures differently than larger, multinational organisations, sometimes with more agility. But the overall accountability architecture, as suggested by the CIPL Accountability Framework, can be the same, irrespective of their size and industry sector. **The ANPD should encourage organisations of all sizes to be accountable and should promote the use of accountability frameworks such as the CIPL Accountability Framework (see figure below) for SMEs and larger organisations to structure their data governance programmes**. The CIPL Accountability Framework is a well-established architecture to build and organise an effective data governance programme that translates legal requirements of the LGPD and other data protection laws into actionable controls. It also enables organisations to be systematic and measure their data governance programme and accountability journey and improve over time.

	 Leadership and Oversight Risk Assessment Policies and Procedures Transparency Training and Awareness Monitoring and Verification Response and Enforcement Accountability Effective compliance, business sustainability, protection for individuals *Figure: the CIPL Accountability Framework* See for reference the following CIPL papers and other resources on the concept of accountability: • Top Priorities for Public and Private Organizations to Effectively Implement the New Brazilian General Data Protection Law (LGPD) (1 September 2020) • What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework (27 May 2020) • The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society (23 July 2018) • Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability (23 July 2018) • Organisational Accountability - Past, Present and Future (30 October 2019)

	• In May 2020 during her Keynote remarks at the Privacy + Security Academy conference, FTC Commissioner Christine Wilson presented accountability as a privacy best practice that is particularly relevant for designing data privacy management programs, relying on CIPL's extensive work on accountability. She also explained the seven elements of the CIPL Accountability Framework and recommended that companies evaluate their data governance programs in light of these elements. See for reference the following CIPL papers on effective regulation: • The Role of the Brazilian Data Protection Authority (ANPD) under Brazil's New Data Protection Law (LGPD) (16 April 2020) • Regulating for Results: Strategies and Priorities for Leadership and Engagement (25 September 2017 (Updated on 10 October 2017) See other CIPL papers: • Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy (25 September 2017) • CIPL Q&A on Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) (19 March 2020) • Certifications, Seals and Marks under the GDPR and Their Roles as Accountability Tools and Cross-Border Data Transfer Mechanisms (12 April 2017)
What are the opportunities related to this topic?	There are a number of opportunities for the ANPD specifically in the context of its upcoming rules on SMEs: • LGPD is focused on protecting the rights and freedoms of individuals and recognises that all parties involved in the processing of personal data in the ecosystem have some level of responsibility and accountability to ensure those rights and freedoms are protected, including SMEs. **The ANPD has an opportunity to encourage that accountability is maintained across the ever more complex data ecosystem/digital supply chain**, which includes controllers, processors and sub-processors within and beyond Brazilian borders. This would, in turn, support building a data protection culture in Brazil, as well as foster digital economic development and innovation; • **The ANPD has an opportunity to position itself as a leading and forward-thinking authority** within Brazil (in relation to authorities of other regulated areas such as consumer and competition) and outside of Brazil (in relation to its peer data protection regulators, in particular within the Latin American region); and

	• **The ANPD has an opportunity to be seen as a constructive regulator** that is open to engaging with regulated organisations, including SMEs, and obtaining their inputs and feedback in order to generate pragmatic and effective guidance.
What are the international experiences regarding this topic?	Many data privacy regulators around the globe have issued guidance and tools to support SMEs' data privacy compliance. Below, CIPL has added links to guidance and tools provided by regulators that we believe are forward-thinking, risk-based and outcomes-based: • The **UK Information Commissioners' Office (UK ICO)** has a webpage dedicated to SMEs, a short guidance to SMEs called "Getting it right: a brief guide to data protection for small businesses" and the UK ICO's Accountability Framework; • The **US Federal Trade Commission (FTC)** also has a webpage dedicated to providing guidance to small businesses; • Equally, the **Office of the Privacy Commissioner of Canada (OPC)** has a webpage with tips and tools to help small businesses address privacy; • The **Singapore Privacy Commissioner (Singapore PDPC)** provides a number of tools to support SMEs kick-start their data protection compliance journey; • The **Hong Kong Privacy Commissioner (HK PDPC)** has published three guidance documents for SMEs: (i) From Principles to Practice – SME Personal Data Protection Toolkit (June 2020), (ii) Data Ethics for Small and Medium Enterprises (April 2019), and (iii) Data Protection & Business Facilitation - Guiding Principles for Small and Medium Enterprises (December 2017); • The **Ireland Data Protection Commissioner (Irish DPC)** has published guidance to SMEs; and • The **Guernsey data privacy regulator (ODPA)** published in 2018 a pragmatic open letter to small businesses and charities in the context of this country's data protection reform acknowledging that this may cause increased pressures on them and that they do not always have the resources or skills at their disposal that larger organisations do, and pointing them to the ODPA's resource centre.
What criteria should be considered in defining SMEs	This question seems to cover two separate concepts: (i) the concept of SMEs and (ii) the concept of controllers and processors. Regarding (i) the concept of SMEs for the purposes of applying any LGPD rules, there are a number of criteria that the ANPD could consider such as number of employees, annual revenue, volume of data processed, and types of data processing activities. In any

that are data controllers and operators?	case, **the ANPD should apply a risk-based approach to its rules concerning SMEs and require organisations to implement more robust technical and organisational measures to protect personal data where their data processing activities represent higher risks to individuals, regardless of the organisation's size**. The ANPD should provide flexible and future-proof guidance concerning risk assessments, as well as examples of data processing activities that may result in higher risks to individuals (e.g. processing involving sensitive personal data or data relating to children, processing involving new technologies), but should also make clear that any risk assessments should be made on a case-by-case basis taking into account all circumstances involved. Regarding (ii) the concept of controllers and processors, it is important that, for consistency and legal certainty, **the same LGPD criteria regarding the definition of controllers and processors should apply to all organisations, regardless of their size**. Article 5, VI and VII of the LGPD define: • Controllers as "natural person or legal entity of either public or private law in charge of making the decisions regarding the processing of personal data"; and • Operators as "natural person or legal entity of either public or private law that processes personal data on behalf of the controller". Therefore, SMEs who make decisions regarding the processing of personal data should be characterised as controllers and SMEs who process personal data on behalf of controllers should be characterised as operators. **The ANPD might decide, however, to clarify the concepts/definitions of controller and operator under the LGPD separately, and that it remains flexible and future-proof when doing so**. See for reference the following CIPL paper regarding the roles of controllers and processors (operators) under the GDPR: • CIPL Response to the EDPB's Guidelines on the Concept of Controller and Processor in the GDPR (19 October 2020)
How has the EU addressed compliance of SMEs with the General Data Protection Regulation (GDPR)?	In its contribution to the evaluation of the GDPR under Article 97 (18 February 2020), the European Data Protection Board (EDPB) has acknowledged that the implementation of the GDPR has been challenging, especially for small actors, most notably SMEs. It is committed to facilitating the development of tools by EU data protection authorities that further alleviate the administrative compliance burden of SMEs. **The EDPB emphasised that in any case, the GDPR risk-based approach should be maintained, as risks for data subjects do not depend on the size of controllers** (note, for instance, that specific GDPR obligations such as appointing a DPO and performing a DPIA are dependent on risk factors such as the scale and nature of the processing and not the

size of the organisation). Finally, it included a very extensive list of guidance, tools and initiatives that such EU authorities have taken with regards to SMEs (see pages 35-45 of the EDPB contribution).

The EDPB has also included specific actions in the EDPB Strategy 2021-2023 (15 December 2020) aiming at facilitating GDPR compliance, including by SMEs. These actions are:

- Providing further guidance on key notions of EU data protection law through the organisation of dedicated stakeholder events and public consultations (including large companies and SMEs, NGOs, DPOs networks and other data protection professionals);
- Further promoting the development and implementation of compliance mechanisms for controllers and processors, in particular codes of conduct and certifications, such as through dedicated workshops and staff trainings; and
- Fostering the development of common tools for a wider audience and engaging in awareness raising and outreach activities, in particular concerning tools specifically tailored for non-expert professionals, such as SMEs, and for data subjects.

In addition, the EU Commission multi-stakeholder expert group, which has a mandate to assist the EU Commission in identifying the potential challenges in the application of the GDPR and advising on how to address them, also issued a report on the evaluation of the GDPR under Article 97 (17 June 2020). The expert group identified a series of challenges concerning the applicability of the GDPR by SMEs, including:

- SMEs generally lack the necessary human and economic resources to implement GDPR obligations, hence they turn to standard solutions (easy compliance instruments and templates) offered either by associations or private firms;
- SMEs have spent considerable resources to adapt to GDPR obligations, such as documentation or establishing data processing policies, which they perceive as an increase in administrative duties;
- Many SMEs had to seek advice from external consultants to understand the GDPR rules and set up systems to comply with the GDPR;
- SMEs have not yet reached an adequate awareness of the need for free consent and what are the consequences of data processing based on “tied consent”; and

	• SMEs have reported difficulties in implementing rules concerning data retention periods, security measures, international transfers and processing DPIAs. The EU Commission multi-stakeholder expert group has also identified a series of mechanisms that could support SMEs in their GDPR compliance efforts: • Concrete guidance and tools, such as templates, to help them apply the GDPR in practice; • Standard contractual clauses to enable international transfers of personal data, as SMEs would not need to negotiate individual contracts; and • Codes of conduct. Finally, the GDPR notably exempts organisations with fewer than 250 employees from their obligation to maintain records of processing activities, unless the processing (i) is likely to result in a risk to the rights and freedoms of data subjects, (ii) is not occasional, or (iii) includes sensitive data or data relating to criminal convictions and offences (Article 30, 5, GDPR). Even though the goal of the EU legislator was to release some administrative burden from SMEs, the legislator also applied a risk-based approach to this exemption. In practice, very few organisations will be able to rely on such exemption, as any processing of personal data may imply "a risk to the rights and freedoms of data subjects". This challenge was also acknowledged by the EU Commission multi-stakeholder expert group in their report mentioned above. See for reference the following CIPL papers: • GDPR One Year In - Practitioners Take Stock of the Benefits and Challenges (31 May 2019) • CIPL Response to the EU Commission's Public Consultation on the Evaluation of the GDPR (28 April 2020)
What are the impacts for SMEs of maintaining records of processing activities?	The LGPD requires controllers and operators to keep records of processing activities (Article 37) and does not provide details on what such records should entail. Maintaining formal records of data processing activities may be burdensome depending on the organisation's level of data processing, in particular for SMEs that have limited resources. However, it is important that organisations understand their data lifecycle and processing activities as this will (i) serve the basis for their risk-based approach, accountability and LGPD compliance efforts, and (ii) enable them to innovate and to identify new business opportunities involving responsible data use.

	The ANPD should therefore not exempt SMEs from maintaining records of processing activities. Rather, the **ANPD should apply a flexible and broad interpretation to the LGPD requirement concerning records of processing activities, avoiding prescriptiveness and focusing on the outcomes of organisations understanding which data they collect, the data lifecycle and their processing activities**. The ANPD could provide templates to SMEs of simplified ways they can maintain records of processing activities, tools available in the market, and how they can merge this activity with other related activities (e.g. defining the legal bases for processing and undertaking risk assessments) for efficiency purposes.
What are the impacts for SMEs of designating a data protection officer?	Article 31, §3º of the LGPD provides that the ANPD may establish complementary rules in relation to the definition and competencies of the DPO, including exemption cases in accordance with the nature and size of the organisation, as well as with the volume of the data processing operations. From an SME point of view, this possibility of the ANPD exemption is welcome. In most cases, SMEs have limited resources and it may be too burdensome to require them to appoint a DPO (in particular in light of lack of ANPD guidance concerning this role, which raises questions such as whether the DPO should be a full-time dedicated position or could be a part time role). However, **CIPL recommends that the ANPD apply a risk-based approach to allow for exemptions concerning appointment of DPOs by SMEs** as well as by start-ups, NGOs and universities that may have extensive processing operations but limited resources. For example, the ANPD could establish that SMEs with low-risk processing activities designate a point of contact for such activities, and SMEs with higher-risk processing activities appoint a DPO (e.g. if the organisation conducts relevant processing of sensitive personal data or children's data, processing in large scale, complex processing activities, or complex structures involving data processing). The obligation to appoint a DPO must be assessed on a case-by-case basis by the organisation based on a set of exemplary criteria such as risk of processing operations, whether or not sensitive data is processed, volume of data processing, etc. Nevertheless, **the ANPD should clarify in its guidance that all organisations, including SMEs, should allocate responsibility for their LGPD compliance activities and their data governance program to an appropriate individual within the organisation, even if he/she works in a different role and not formally fulfils the DPO role**. Also, as we mention further in this CIPL response, the ANPD should provide guidance and examples to support SMEs and other organisations in conducting risk assessments. ANPD's guidance should also be outcomes-based – i.e. it should **encourage a flexible interpretation of the LGPD DPO requirements to enable SMEs achieve the best possible outcomes in protecting personal data within their specific context and circumstances** including their size, type of organization, type of data processing

	activities, and resources or lack of resources. In particular, ANPD's guidance should cover the following topics that are key to enable flexibility for SMEs concerning the appointment of a DPO: • **Full-time vs. part-time DPOs** – differently than the GDPR, the LGPD does not have specific requirements concerning DPO independence and conflicts of interest, which enables flexibility concerning the appointment of DPOs who also fulfil other roles under the organisations. For many SMEs, having a part-time DPO would be more appropriate than a full-time DPO, as often there is only one person responsible for legal and compliance or other activities that are related to data processing and the role of the DPO; and • **Internal vs. external DPOs/"DPO as a service"** – generally, the external DPO may be particularly appropriate for SMEs (although it may be too expensive for most) as it would ensure that they have the required level of data protection expertise and knowledge available to their organisations without incurring substantial administrative and financial burdens typically associated with hiring a full-time employee (e.g. SMEs and start-ups would only have to remunerate the external DPO for his/her hours of work). However, in some cases internal DPOs may be more appropriate even for SMEs. This may be the case where the organisation's data processing operations are complex, dynamic and fast-moving, in which case they may need a responsible person in-house who is fully integrated in the business and hence has a good understanding of it. For example, SMEs, and in particular start-ups, might need someone working with them more intensely in the beginning of their establishment as a business to help them set up their services, and then have someone more part-time to make sure data privacy is addressed in an ongoing basis. Hence, it is important that the ANPD provides flexibility for SMEs in relation to the appointment of the role of the DPO and clarifies the circumstances SMEs will be exempt from the formal appointment obligations. Even if exempt, some SMEs may decide to appoint a DPO for strategic, business reasons (e.g. enhance consumer/client trust, enhance competition powers). SMEs that are operators may also want to appoint a DPO for the same reasons. Appointing a DPO should be seen as best practice and a way for organisations to demonstrate accountability, as data governance is one of the key enablers of responsible uses of personal data. Therefore, **the ANPD should encourage the appointment of a DPO or a person with equivalent responsibilities for all organisations, including SMEs, even when they are exempted from such appointment or characterised as an operator**. Finally, **the ANPD should also encourage the creation of a DPO network/community** in Brazil. This could be specific for industries, size, and regions in Brazil. Such a network/community would be particularly relevant for SMEs as it would enable

	sharing of information, good practices and benchmarking, which would facilitate DPO training and ultimately enhance LGPD compliance among SMEs. See for reference the following CIPL papers regarding the role of the DPO under the GDPR: • Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation (17 November 2016) • The Role of the Data Protection Officer (DPO) and Risk and High Risk under the GDPR (5 October 2016)
What are the impacts for SMEs of producing data protection impact assessments?	DPIAs are one of the mechanisms organisations can use to assess the risks relating to their data processing activities, which are drivers of wider accountability (see our response to the question "What are the impacts for SMEs of establishing a systematic assessment of risks to privacy and data protection?"). The LGPD does not explicitly require organisations to undertake DPIAs, except when the ANPD requires it (Article 10, paragraph 3 and Article 38). Also, the LGPD does not provide many details on what DPIAs should entail, except that they should describe the personal data processed, the methodology used for collection and ensuring data security as well as for the risk analysis, and any safeguards and risk mitigation measures. **The ANPD should reach a balance between providing guidance and templates to SMEs concerning risk assessments (including DPIAs), maintaining the LGPD's flexibility on this topic and avoiding overly-prescriptive rules**. The ANPD should encourage SMEs to undertake risk assessments, including DPIAs, in the form and circumstances that are more appropriate to their organisation, as long as they result in the desired outcome of analysing the risks to individuals and mitigation measures implemented to mitigate such risks—there may be instances where SMEs may therefore be excused from undertaking full DPIAs. The actual process or methodology of risk assessments and DPIAs should largely be left to individual organisations. Any ANPD guidance on the risk assessment process or methodology should therefore be principles based, high-level and flexible. The ANPD could provide templates to SMEs and other organisations of DPIAs if they require them to undertake this particular type of risk assessment, but it should make it clear that such templates are voluntary and organisations can use other templates and methodologies appropriate to their context as long as they fulfil the requirements of Article 38 of LGPD. The ANPD should also provide examples to SMEs of which cases the ANPD may require them to undertake full DPIAs. See the following CIPL paper on risks and DPIAs: • Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (21 December 2016)

What are the impacts for SMEs of complying with the LGPD rules concerning data processing, including of sensitive data and data of children and teenagers?	The LGPD rules concerning data processing apply equally to controllers and operators regardless of their size. LGPD has specific rules concerning processing of sensitive data and data relating to children and teenagers (Articles 11 to 14 LGPD), which SMEs must also observe. In addition, the ANPD must require SMEs to apply a risk-based approach to their data processing activities, which will include possibly applying more robust technical and organisational measures to processing of these types of data, as they are likely going to present a higher level of risk to the individuals concerned.
What are the impacts for SMEs of implementing a data governance program?	As outlined in our response to the question "What are your suggestions for addressing these problems?" above, data governance programmes are scalable and therefore can be implemented by SMEs, who calibrate the programme requirements according to their context, risks and goals. Implementing data governance programmes generate a number of benefits for SMEs and more generally for the Brazilian economy: • **SMEs become more attractive as vendors/operators to controller organisations**, including larger and international organisations – the implementation of data governance programmes is an indication of accountability, which drives business opportunities by ensuring eligibility for business partnerships that involve personal data. Organisations engaging in data processing activities that depend on vendors/operators also need to ensure that personal data is processed when transferred to such vendors/operators. They do so by assessing the risks of vendors and implementing appropriate contractual clauses. The risks relating to data protection are likely to be smaller, and negotiating data protection contractual clauses will take less effort, if vendors have appropriate protective measures in place, including a data governance programme; • **SMEs may use their data governance programme as a competitive differentiator** – they may have a competitive advantage over other SMEs given that not only do they become attractive as vendors/operators (see point above), but also they may decide to use their data governance programme as part of their branding strategy (e.g. by saying they have robust mechanisms in place to protect individuals' personal data). If they are consumer-facing SMEs, they may use this also to enhance consumer trust; • **SMEs' risk of LGPD non-compliance and possible ANPD sanctions will decrease** – as data governance programmes equip SMEs with policies, processes and mechanisms to comply with the various LGPD rules. This will prevent enforcement actions or, in the event of enforcement, possibly streamline and reduce the financial impact of such enforcement given that the SME would be equipped to demonstrate compliance efforts to the ANPD;

	• **Encouraging organisations of all sizes to implement data governance programmes will ultimately increase trust in the Brazilian data ecosystem and enable data-driven innovation** – this will foster the Brazilian digital economy and prevent that individuals stop using online services out of fear, for instance, of their personal data being subject to breaches. It will help enhance trust with other stakeholders such as media, investors, the ANPD, customers and employees; • **Encouraging organisations of all sizes to implement data governance programmes will also enable data-driven innovation** – increased compliance with LGPD rules means that SMEs will be able to extract value of personal data while using it in a responsible, accountable and compliant manner, which will enable them to innovate through data processing; and • **Encouraging organisations of all sizes to implement data governance programmes will also likely decrease the number of data breaches notified to the ANPD** – a key element of data governance programmes is the implementation of systematic risk assessments. These enable organisations to more effectively and efficiently detect and mitigate data breaches. Ultimately, the ANPD is likely to receive less notifications of data breaches that "can result in relevant risk or harm to data subjects" (Article 48, LGPD), as organisations will be better equipped to prevent such risks and harms from occurring.
What are the impacts for SMEs of establishing data security policies?	The ANPD should not grant exemptions to SMEs in relation to establishing and implementing data security policies and related processes. This is particularly important as the COVID-19 crisis has triggered an acceleration of digital interactions and activities among all organisations including SMEs, which leaves them more vulnerable to cyberattacks as well as data breaches. Implementing data security measures is important not only to protect individuals, but also to protect SMEs' assets and business. Rather, the **ANPD should require SMEs to implement data security policies, processes and tools (measures) according to the level of risk of their data processing activities to individuals and society**. These measures should be flexible, adaptable and future-proof and not locked into the current state of the art in data security. The ANPD should work with industry to identify and provide to SMEs examples of different types of data security measures (including anonymisation and pseudonymisation), as well as case studies demonstrating how such measures can be applied to mitigate different types of risks and harms. It should also be guided by the existing international data security standards, such as the PCI Payment Card Industry standards and the different ISO data security standards (see here and here), as these are already commonly used globally and will be recognised by larger organisations with which Brazilian SMEs work as vendors or business partners.

What are the impacts for SMEs of establishing a systematic assessment of risks to privacy and data protection?	Risk assessment is one of the core elements of organisational accountability and the **ANPD should include it as a key element of its upcoming rules and guidance concerning SMEs**. Risk assessment means balancing the interests of the organisation and society against the possible harms to individuals, and mitigate risk in ways that are appropriate to the context. Risk assessments include managing privacy risks at various levels, as appropriate: (i) data governance programme, (ii) processing activities, products, services, technologies and applications, (iii) use of vendors and third parties, (iv) contextual risk assessments such as legitimate interests assessments and DPIAs, (v) calibration and periodic review of these various types of risk assessments in light of changes in business models, law, technology and other internal and external factors. It is key for SMEs to be able to undertake risk assessments, as these will enable them to (i) make informed decisions, (ii) prioritise their activities and resources, and (iii) apply context-appropriate and risk-based privacy protections regardless of the specific technology or practice that is being assessed.
What are the impacts for SMEs of data portability?	Data portability is a key enabler of the digital economy. It allows for individuals to promptly move their personal data from one service to another instead of being "locked" into a particular service provider. This right can work as an enabler of digital trust, competition and economic growth, particularly for SMEs. **The ANPD should work with multiple stakeholders, including industry sectors and other Brazilian regulators, to understand and maximize the benefits and opportunities of data portability for individuals and organizations, including SMEs**. ANPD's regulation on data portability has the potential to drive the standardization of interoperability rules related to personal data. This will result in efficiency gains to the Brazilian digital economy, better and diversified services for consumers, and the accomplishment of this data protection right. Besides providing further rules for SMEs, the ANPD is entitled to issue specific regulations on how to implement the right to data portability (Article 18, V of the LGPD). When providing such regulations, the ANPD should work with industry to understand their challenges and needs concerning the development of common sets of interoperable standards and formats and the costs involved in implementing them, security of data transmission, data quality, types of data to be ported, as well as competition and intellectual property issues.
What regulatory mechanisms could be used to promote	There are a number of regulatory mechanisms that the ANPD could use to promote innovation by SMEs: • **Undertaking regulatory sandboxes** – given the remarkable transformation of our societies and economies as part of the fourth industrial revolution, it is critical that Brazil enables data-driven innovation while ensuring responsible use of data

and incentivise innovation by SMEs?	and protection of individuals' rights and interests. Regulatory sandboxes could provide a safe space where SMEs can innovate through responsible uses of personal data under the supervision and advice of the ANPD. The ANPD should consider the various types of regulatory sandboxes it could undertake: (i) focused on a specific data protection challenge (e.g. artificial intelligence), (ii) focused on a specific industry (e.g. fintech sector), and (iii) in a cross-sectoral manner in partnership with other regulatory authorities to the extent that data protection challenges cut across various regulated areas (e.g. consumer, competition, banking, telecommunications); • **Promoting the development of industry codes of conduct, certifications, seals and trust marks** – as they are promising instruments for data protection and to enable tackling hard questions and challenges that are specific to a particular industry, demonstrating accountability as well as sharing of industry best practices, which is particularly relevant for SMEs; • **Enabling data sharing** – the importance of sharing of personal data between government and organisations has become more prominent in the context of the COVID-19 pandemic, with numerous examples of research institutions and universities (normally characterised as SMEs) seeking access to personal data to undertake relevant analysis and support finding solutions. Access to data and being able to use data is a necessity for innovation, and it is particularly relevant to SMEs as they naturally have access to less personal data compared to larger, more competitive and technologically advanced organisations. The ANPD should facilitate and promote data sharing in the context of the LGPD by establishing rules and providing guidance on data sharing as per Article 11, paragraph 3 and Article 30 of the LGPD. See for reference the following CIPL papers: • Regulatory Sandboxes in Data Protection - Constructive Engagement and Innovative Regulation in Practice (8 March 2019) • CIPL Response to the EDPB's Guidelines on Codes of Conduct and Monitoring Bodies under the GDPR (29 March 2019)
SUGGESTIONS OF PROVISIONS	
CIPL does not have specific suggestions of provisions.	