Paper 2 of the Joint Project

"Effective Implementation and Regulation Under the New Brazilian Data Protection Law"

Top Priorities for Public and Private Organizations to Effectively Implement the New Brazilian General Data Protection Law (LGPD)

Centre for Information Policy Leadership (CIPL) and

Centro de Direito, Internet e Sociedade of *Instituto Brasiliense de Direito Públic*o (CEDIS-IDP)

1 September 2020

This is the second paper of the special Joint-Project "Effective Implementation and Regulation Under the New Brazilian Data Protection Law (LGPD)", by CIPL and CEDIS/IDP.[i] This project strives to: facilitate information-sharing about the LGPD; inform and advance constructive, forward-thinking and consistent LGPD implementation; enable the sharing of industry experience and best practices; and promote effective regulatory strategies concerning the LGPD–more information and the materials produced as part of this project can be found at <https://www.informationpolicycentre.com/brazilian-data-protection-implementation-and-effective-regulation.html>.[ii]

Contents

Checklist: Priority Steps for LGPD Compliance

Priority 1. Understand the LGPD impact on the organization and obtain buy-in from top management

- ☐ Understand the impact of the LGPD rules on the organization and its use of personal data as a controller and/or operator.
- ☐ Explain and demonstrate to senior management the importance of privacy compliance and the benefits of accountability.
- ☐ Request support from senior management, including budget and resources.

Priority 2. Designate a person in charge of data protection, and identify and engage key stakeholders

- ☐ Designate the organization's DPO and document and communicate their role and responsibilities internally.
- ☐ Identify and engage key internal stakeholders and senior leaders who will sponsor the data privacy management program and who will own program implementation activities.
- ☐ Identify and engage with key external stakeholders.

Priority 3. Identify the organization's processing activities and the data that the organization handles

- ☐ Define the methodology to map and record the organization's processing activities (as controller and/or operator) and periodically review the data lifecycle.
- ☐ Map the organization's data and processing activities as soon as possible.
- ☐ Consider anonymization and data minimization to reduce the organization's risk and compliance burden.

Priority 4. Determine the organization's role and obligations as a controller or operator

- ☐ Determine the organization's role and obligations as a controller or operator.
- ☐ Communicate these obligations to the relevant individuals and teams within the organization.
- ☐ Consider any updates needed to standard customer contracts to reflect the organization's role.

Priority 5. Assess the privacy risks associated with the organization's data processing

- ☐ Implement a data privacy risk assessment process that includes consideration of risks to individuals.
- ☐ Prioritize compliance measures related to data processing that carries the highest risks for individuals and the organization.

Priority 6. Design and implement a data privacy management program covering the LGPD requirements

- ☐ Design a data privacy management program and an action plan for implementing it based on the identified risks.
- ☐ Identify easier tasks and implement them as soon as possible.
- ☐ Maintain and review the data privacy management program on an ongoing basis.

Priority 7. Define the legal bases for the organization's data processing activities

- ☐ Identify the individuals or team that will be responsible for determining the legal bases for processing—they should define the legal bases the organization relies upon as a priority.
- ☐ Consider what processes should be put in place and/or adapted for ongoing maintenance of the legal bases for processing activities.

Priority 8. Define technical and organizational measures for effective data security and internal reporting and management of security incidents

- ☐ Work with the information security and systems/data architecture teams to determine the changes needed to implement appropriate data security measures.
- ☐ Establish a process for internal reporting and managing of security incidents and personal data breaches and notifying the ANPD if necessary.

Priority 9. Identify all third parties with which the organization shares personal data and establish a third party management process

- ☐ Identify the third parties that process personal data on the organization's behalf, and determine whether it processes personal data on behalf of another organization.
- ☐ Assess and adopt third party management mechanisms, including due diligence and entering into data processing agreements.

Priority 10. Identify the organization's cross-border data flows (inbound and outbound) and put in place appropriate data transfer mechanisms and safeguards

- ☐ Identify whether the organization transfers personal data to third countries, for what purposes and in what capacity (as controllers and/or operators).
- ☐ Assess and implement the transfer mechanisms that are most appropriate for the organization.

Priority 11. Build effective processes for transparency and data subject rights

- ☐ Prepare privacy notices and other relevant resources to provide easily accessible information to individuals about the organization's data processing.
- ☐ Map the various case scenarios for data subject rights requests and assess the organization's response time to requests to develop the relevant processes.
- ☐ Develop processes to respond to such requests.

Priority 12. Train employees on LGPD requirements and create an awareness-raising program

- ☐ Implement ongoing training for all existing employees, contractors and new-joiners.
- ☐ Plan training and communications activities both in the beginning of the organization's data privacy management program and on an ongoing basis.

Top Priorities for Public and Private Organizations to Effectively Implement the New Brazilian General Data Protection Law (LGPD)

I. INTRODUCTION

The new Brazilian data protection law (*Lei Geral de Proteção de Dados Pessoais*—LGPD)[iii] brings new data protection concepts and rules to Brazil, which did not previously have a comprehensive data privacy law in place. Such rules will apply to both public and private sector organizations, regardless of where they are located, if they fall within the scope of the law.[iv]

Some organizations have already made notable progress towards LGPD compliance. However, many organizations are still in the very early stages of implementing the LGPD's requirements. This paper intends to help these organizations define and prioritize the steps they need to take to implement the LGPD effectively.

The actual compliance program and measures that organizations build and implement will depend on a number of variables, including an organization's size, sector, geographic reach and type of business, as well as the volume, nature and risk level of its data processing operations. Further, as noted, organizations are at different stages of progress towards compliance, both within Brazil's and global privacy laws. Moreover, Brazilian-based organizations, particularly small and medium size enterprises (SMEs), will likely have to implement a greater number of new compliance measures than Brazilian affiliates of larger, foreign-based organizations, which will be able to leverage their existing global data governance programs to comply with the LGPD.

Finally, under the LGPD, the new data protection regulator, *the Autoridade Nacional de Proteção de Dados Pessoais* (ANPD) is charged with numerous regulatory tasks that will inform, guide and impact the specific compliance and implementation steps taken by organizations.[v] However, as a brand new data protection authority, the ANPD will need time before it can provide guidance on all necessary LGPD provisions[vi]. Each of the above factors may impact the selection and prioritization of the implementation actions we suggest in this paper.

II. ORGANIZATIONAL PRIORITIES FOR LGPD IMPLEMENTATION

Priority 1. Understand the LGPD impact on the organization and obtain buy-in from top management

While the impact of the LGPD differs from one organization to another, **all organizations must understand the importance of being accountable for how they process personal data**. Accountability is one of the core principles of the LGPD[vii] (Article 6, X and Article 50) and applies to both controllers and operators (see Priority 4). It means that organizations (i) take steps to translate data privacy legal requirements into risk-based, concrete, verifiable and enforceable actions and controls through the implementation of comprehensive data privacy management programs and (ii) are able to demonstrate the existence and effectiveness of such actions and controls internally and externally.

Accountability begins with ensuring that top management understands the business value of privacy and the potential ramifications of the failure to comply. This first step of obtaining leadership buy-in is necessary to secure the strategic alignment and resources that will be required to implement

accountability and ensure compliance. This will also enable senior leadership to understand the privacy risk profile of their organization and make informed decisions about personal data processing, taking into account the core activities, business priorities, ambitions and values of the organization (see Priority 5). Health care providers, for instance, may have a higher privacy risk profile, particularly in the context of COVID-19, which would trigger more in-depth privacy assessments and controls and a greater need for assistance and resources.

Therefore, **top management must understand that investing in a data privacy management program will be beneficial to the organization** because it would:

- Allow compliance with legal and regulatory requirements and enable trustworthy data processing activities, including given the reduced exposure to risk of LGPD non-compliance;
- Instill a privacy-conscious culture within the organization;
- Help the organization provide better privacy protection for its customers, which impacts customer acquisition and retention;
- Drive business opportunities by ensuring eligibility for business partnerships that involve personal data;
- Help enhance trust with other stakeholders such as media, investors, regulators, customers and employees;
- Preserve competitive advantage and enable differentiation; and
- Prevent enforcement actions or, in the event of enforcement, streamline and reduce the financial impact of such enforcement given that the organization would be equipped to provide evidence of its compliance efforts to the ANPD.

Prior to making the case for privacy compliance and accountability to top management, individuals responsible for LGPD compliance within an organization should first consider the following questions:

- How does the LGPD apply to the organization and what are its requirements?
- What are the data processing activities of the organization? How critical are they to its core business activities?
- How much effort (e.g., budget, time and personnel) is needed by the organization to align with the LGPD's standards?
- What requirements are new compared to other applicable Brazilian laws and sectoral regulations (e.g., Consumer Code, the Brazilian Civil Rights Framework for the Internet—*Marco Civil da Internet*)?
- What requirements are new compared to other international laws to which the organization is subject in other jurisdictions (e.g., the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Personal Information Protection and Electronic Documents Act (PIPEDA))? What can be extended to Brazil operations for LGPD compliance purposes? This question does not apply to organizations that solely operate within the Brazilian territory and only process personal data of Brazilian individuals.
- Does the organization already meet some of the LGPD requirements (including through contractual obligations)?

- Can the organization leverage internal processes and existing data privacy management programs to meet the new LGPD requirements, such as risk management, project management, information security and data governance structures?
- How much would it cost (including hiring personnel, investing in technology, upgrading IT systems, etc.) to put in place a data privacy management program to close identified gaps in compliance?
- What would be the impact of non-compliance with the LGPD on the organizations' revenues, reputation, brand and client trust? What could be a potential LGPD fine for the organization for non-compliance?
- Are there any tangible business opportunities in implementing the LGPD (e.g., enhancing user trust, selling a new product, outperforming competitors, making internal and external processes more efficient)?
- What are the organizations' stakeholder's (e.g., consumers, partners, clients, shareholders) expectations in terms of compliance with the LGPD?

Performing a gap assessment in the early stages of privacy compliance could help organizations determine how much more implementation activity is needed to reach baseline LGPD compliance (or any higher privacy goals the organization may have) from the organization's current level of privacy maturity. The results of these assessments should constitute a solid basis for designing their data privacy management programs and estimating their costs.

Presenting top management with facts and figures will also help get their buy-in. The Cisco Data Privacy Benchmark Study 2020,[viii] for instance, makes the case for privacy return on investment (ROI), by demonstrating that there are strong correlations between organizations' privacy accountability and lower breach costs, shorter sales delays, and higher financial returns. It also shows that more than 40% of organizations globally are seeing benefits at least twice that of what they spend on privacy. What would also help make this point would be a few use cases and examples of enforcement sanctions and how these have impacted organizations' business and reputation in the market. The *Netshoes,*[ix] *Banco Inter*[x] and *Drogaria Araújo*[xi] cases, for instance, may be instructive.

Once the relevant staff leading LGPD compliance internally have achieved this high-level understanding of the LGPD requirements, their impact on the organization, and the necessary steps to achieve compliance, the staff will be equipped to present them to top management and ask for the budget and resources to implement a data privacy management program (see Priority 6).

Key steps for consideration:

- Understand the impact of the LGPD rules on the organization and its use of personal data as a controller and/or operator.
- Explain and demonstrate to senior management the importance of privacy compliance and the benefits of accountability.
- Request support from senior management, including budget and resources.

Priority 2. Designate a person in charge of data protection and identify and engage key stakeholders

Data protection officers

The LGPD requires controllers to appoint a person to be in charge of the organization's data processing activities (Article 41), which, in practice, means their data privacy compliance and data privacy management program. In this paper, we will refer to this role as the Data Protection Officer (DPO). The DPO will:

- Work as the main point of contact between the controller, data subjects and the ANPD (Article 5, VIII);
- Be responsible for acting upon data subject and ANPD requests (Article 41, paragraph 2); and
- Provide advice and guidance to the organization on data protection and LGPD compliance (Article 42, paragraph 2).

DPOs have a key role in the planning, implementation and oversight of controllers' data privacy management programs. They also act as a strategic advisor on the responsible, effective and innovative use of personal data by the controller.

In principle, all controllers are required to appoint a DPO according to the LGPD. Operators may also decide to appoint a DPO given that they are also required to implement measures to ensure data governance (Article 50)—which, in practice, means the adoption of a data privacy management program. The ANPD may provide further requirements concerning DPOs through complementary rules, including exemptions for appointing the DPO based on the nature, size of the organization and the volume of personal data processed (Article 41, paragraph 3).

In order for DPOs to be able to effectively discharge their responsibilities, organizations must provide them with appropriate resources, which will depend on the size and privacy risk profile of the controller. Such resources may include:

- Staffing resources;
- Certification and/or qualification to ensure the DPO has, and maintains, required subject matter expertise in privacy and data protection;
- Compliance technology and tools;
- Access to external legal advice and technical and consultancy advisors;
- An adequate and separate budget for DPO activities, training and staff, and
- Autonomy and independence to perform DPO tasks.

In addition, **organizations should designate DPOs who have at least some expertise in privacy and data protection as well as knowledge about the organization's business model and governance structure**. Based on existing practice, there are certain skills that are essential for DPOs and their teams to effectively exercise their roles. Such skills include:

- Leadership skills;
- Interpersonal and communication skills;
- Organizational and privacy program management skills across multiple departments;

- Analytical skills;
- Business skills, including understanding of the business model and organization infrastructure;
- Technology skills; and
- External engagement skills.

Organizations should designate the DPO, or determine whether their existing global DPO or CPO would also cover the responsibilities under LGPD. **Organizations should also document the role and responsibilities of the DPO and communicate these to all employees in the organization**—for instance, through a DPO Charter or internal policy.

While larger organizations may appoint a full-time, dedicated DPO, this may not be possible for other organizations such as SMEs and start-ups due to resource constraints. Nevertheless, all organizations should allocate responsibility for the data privacy management program and related activities to an appropriate individual, even if he/she works in a different role.

The LGPD does not explicitly require the DPO role to be independent or free of any conflict of interests, but the ANPD may issue further rules concerning this role. However, as a matter of good practice, organizations should avoid assigning a mandate that could be in conflict with the individual's other responsibilities in terms of time allocation or ability to prioritize, and should be able to evidence such rationale.

Data Privacy Management Program Sponsors, Partners and Team

Accountability is a multi-stakeholder effort that has to be run horizontally across the organization. Therefore, in addition to designating a DPO, **organizations should also identify key stakeholders within the organization who would work as the data privacy management program sponsors, partners, and the core program team**. There should be clear roles and responsibilities assigned to each of these stakeholders, as well as clear reporting lines.

Often, these stakeholders form a **cross-functional data privacy steering committee**. Collectively, this group should have deep knowledge of the organization's operations and business to ensure that relevant data-related processes, services and products will be covered by the data privacy management program.

Key business functions that are normally closely involved with data privacy management programs include legal, risk, and compliance and information security. Other business functions will also be key stakeholders in understanding current practices and business needs as well as implementing process updates, particularly if they are involved in the processing of sensitive personal data. These functions will be involved depending on the structure of the organization and its operations, including engineering, product teams, marketing, human resources, and others.

The DPO should engage and obtain buy-in from these stakeholders as soon as possible, given that they will:

- Inform the establishment of the program;
- Inform about any required adaptations of existing programs, systems, policies and processes (e.g. if changes in systems are needed, information security will advise on how long they will take and how much they will cost);

- Help ensure effective ownership of the relevant parts of a program as well as specific actions and controls; and
- Facilitate implementation of the program.

There are many ways that organizations can engage stakeholders in their LGPD program to help define the key work streams and milestones of the data privacy management program—for example, through workshops, periodic meetings with the core program team to review progress on these work streams, and establishing steering committees for decision-makers and program sponsors.

External stakeholders

Finally, **organizations may also identify key external stakeholders, monitor their activities and regularly engage with them**. These stakeholders may provide insights in terms of external data protection developments and LGPD interpretation that may be helpful for organizations' LGPD implementation activities. Some organizations also engage external stakeholders to seek feedback to and to benchmark such activities. Examples of external stakeholders include the ANPD directors and staff (when the ANPD is established), local privacy experts and other organizations of the same industry sector.

Key steps for consideration:

- Designate the organization's DPO and document and communicate their role and responsibilities internally.
- Identify and engage key internal stakeholders and senior leaders who will sponsor the data privacy management program and who will own program implementation activities.
- Identify and engage with key external stakeholders.

Priority 3. Identify the organization's processing activities and the data that the organization handles

Understanding the organization's data lifecycle and processing activities is necessary for compliance with a series of LGPD requirements, including to:

- Ensure the accuracy and relevance of personal data (Article 6, V);
- Assess the risks to individuals relating to their processing activities and for designing and calibrating their data privacy management program (Article 50);
- Identify the relevant legal bases for processing (Article 7);
- Provide the right information to individuals about their processing operations (Article 9, II, V);
- Respond to individual rights requests (Articles 6, IV; Article 18);
- Determine what safeguards to put in place to enable international transfers of personal data (Article 33 and following);
- Establish records of processing activities (Article 37);
- Prepare data protection impact reports (referred to in this paper as data protection impact assessments—DPIAs); and

- Provide related information to the ANPD if required (Article 38).

Many organizations make use of data mapping methodologies and tools. The level of depth of such mapping will depend on the organization's needs as well as the type and volume of their processing activities. Data mapping is not, however, an express requirement of the LGPD. In practice, understanding the data lifecycle and processing activities means that organizations must have a clear overview of:

- What personal data they collect and process and for which purposes;
- On what systems/applications they collect and process personal data;
- Who has access to personal data, who they share it with and why;
- Whether they share personal data internationally; and
- When personal data must be deleted.

Having this understanding and overview of data and processing operations also **benefits organizations from a business perspective**, as it:

- Fosters good data management, security and "data hygiene;"
- Enables organizations to build trust with their employees, customers and partners by enhancing responsible data handling practices and mitigating business risk; and
- Enables organizations to identify opportunities for further uses of data in innovative ways, for instance, through anonymizing the data. Because anonymized data falls outside of the scope of the LGPD (Article 12), anonymization is a mechanism that enables the use of data for a broader range of new purposes.

Key steps for consideration:

- Define the methodology to map and record the organization's processing activities (as controller and/or operator) and periodically review the data lifecycle.
- Map the organization's data and processing activities as soon as possible.
- Consider anonymization and data minimization to reduce the organization's risk and compliance burden.

Priority 4. Determine the organization's role and obligations as a controller or operator

It is important that organizations clearly define their role in data processing scenarios (such as through data processing agreements or specific clauses in general contracts). Under the LGPD, organizations can be controllers and/or operators (Article 5, VI and VII, and Article 39) as well as joint-controllers (Article 42, paragraph 1, I):

- Organizations are **controllers** when they determine the purposes for, and take decisions regarding the use and processing of personal data (such as in respect of their employees, job candidates, customers, business contacts, website, app and other online users). Controllers sometimes use operators to undertake some processing on their behalf. For example, a controller may use a third party to provide payroll services for its employees. Controllers can

also set up operators within the same corporate group, for example, when all entities use an IT help desk run by one of the entities on behalf of the others.

- Organizations are **operators** when they act on the instructions of, and process data on behalf of, controllers. An example would be when an organization provides call center or IT support services to other organizations.
- Organizations can simultaneously be **controllers and operators**. For example, an organization would be a controller if it uses its own resources to process its own customers' personal data, but would also be an operator if it provides IT solutions to other organizations.
- Two or more organizations can be **joint-controllers** when they jointly determine the purposes of personal data processing (and they can also use third parties as operators). For example, when a franchisor and a franchisee jointly determine the means for processing clients' personal data in the context of distribution agreements.

The LGPD responsibilities for controllers and operators vary. Both controllers and operators must keep records of processing activities (Article 37) and ensure the security of personal data (Article 46). There are, however, many more explicit obligations for controllers than for operators (see Appendix 2). Moreover, in many cases, controllers may need the support of operators to perform required activities, such as in the following:

- Undertaking DPIAs and legitimate interest assessments (LIAs) (Article 10, paragraph 3; and Article 38);
- Demonstrating that consent is valid (Article 8, paragraph 2; and Article 14, paragraph 5);
- Providing information to individuals (Article 8, paragraph 6; Article 9, paragraph 2; Article 10, paragraph 2; Article 18; and Article 20, paragraph 1);
- Enabling the exercise of data subject rights (Article 18); and
- Notifying the ANPD about data breaches in case of relevant harms to data subjects (Article 48).

Therefore, **controllers and operators must maintain a trust-based relationship**. The LGPD expressly recognizes that such cooperation is needed, for instance, in order to operationalize data subject rights requests (Article 18, paragraph 3). In fact, the LGPD establishes that, in some cases, both controllers and operators may be liable for damages caused to individuals resulting from processing operations (Article 42), and also provides exceptions to such joint liability (Article 43).

Key steps for consideration:

- Determine the organization's role and obligations as a controller or operator.
- Communicate these obligations to the relevant individuals and teams within the organization.
- Consider any updates needed to standard customer contracts to reflect the organization's role.

Priority 5. Assess the privacy risks associated with the organization's data processing

The LGPD is a risk-based legislation. **Organizations must understand and assess the privacy risks to individuals associated with their processing activities, projects, products and services, and implement tailored controls and mitigations accordingly**. The element of risk to individuals—which could also translate into risks to the organization itself (e.g., liability and reputational risks)—underpins many of its requirements, including:

- Organizations must adopt measures to prevent any harms to individuals resulting from personal data processing activities (Article 6, VIII);
- The LGPD provides that data processing is "irregular" when it does not protect individuals according to risks (Article 44);
- Organizations must calibrate their privacy compliance and governance programs based on risk to individuals (Article 50);
- Organizations must notify the ANPD when security incidents may result in relevant risks and harms to individuals (Article 48);
- The ANPD may require controllers to prepare DPIAs (Article 38) and LIAs (Article 10, paragraph 3); and
- The ANPD may also provide technical standards for security measures and encourage the adoption of industry standards for services and products that facilitate the exercise of individual control over personal data based on risks (Articles 46, paragraph 1 and 55-J, VIII respectively).

There are many ways that organizations can identify, assess and manage data privacy risks.[xii] These include undertaking DPIAs and LIAs, integrating privacy risks assessments within their existing risk management framework, managing risks at the data privacy management program and product/service levels (e.g., through periodic reviews), and assessing privacy risks that are specific to the use of vendors and third parties. SMEs can develop simpler and more agile ways of identifying, tracking and controlling risks.

There are many available methodologies, templates and software solutions that organizations can use to undertake data privacy-related risk assessments and, in particular, DPIAs. See, for instance, the ones provided by the French data protection authority (CNIL),[xiii] the UK Information Commissioner's Office (UK ICO),[xiv] the US NIST Privacy Framework,[xv] as well as automated tools offered by third party service providers such as OneTrust[xvi] and TrustArc.[xvii]

It is important that the DPO is involved in data privacy-related risk assessments. In addition, organizations may need to train specific personnel to support the business to undertake DPIAs and LIAs at scale, as these may require technical privacy knowledge.

Key steps for consideration:

- Implement a data privacy risk assessment process that includes consideration of risks to individuals.
- Prioritize compliance measures related to data processing that carries the highest risks for individuals and the organization.

Priority 6. Design and implement a data privacy management program covering the LGPD requirements

The LGPD requires organizations to put in place privacy compliance and governance programs, which should be calibrated based on risk (Article 50, paragraph 1). The LGPD also details some of the elements that these compliance programs must cover, such as policies and procedures, risk assessments, transparency, and others.

Implementing an accountable privacy compliance program is an iterative and dynamic process that requires organizations to constantly adapt to internal and external factors; address regulatory, legal and technological change; and mitigate new data privacy-related risks. Data privacy management programs can cover only LGPD requirements, or can have a wider scope to cover privacy requirements of other jurisdictions or even apply on a global scale, leveraging compliance efforts organizations have already taken in other jurisdictions.

Organizations of all types, sizes, cultures, sectors (including the public sector) can develop and implement data privacy management programs appropriate to their specific context, risks and goals. While it may be more challenging for SMEs to implement a full fledged privacy program, they can also take steps to organize and structure their privacy compliance effort, sometimes in a more agile manner than bigger organizations depending on the types of personal data they process. Notably, the ANPD can establish more flexible rules for SMEs, depending on the risks associated with their processing activities (Article 55-J, XVIII).

Organizations should go through a series of steps to set up and implement their data privacy management programs as appropriate to their internal structure, privacy maturity level and risks (see Priority 5). While some of these steps are outlined below, they are illustrative and not comprehensive:

- Identifying the organization's LGPD compliance gaps (see Priority 1);
- Designating individuals to be responsible and accountable for the program and to support with program implementation (see Priority 2);
- Defining the scope of the program, program workstreams, milestones and external or internal dependencies (such as with existing IT and information security), with consideration to the necessary and available time to implement these items, as well as budget, resources and required technology or process changes;
- Identifying easy tasks that can be implemented immediately;
- Developing an action plan including specific actions to reach each of the milestones, ownership for implementation, and priorities (e.g., developing or updating internal policies, processes and procedures, templates, training programs, updating contracts) and tracking implementation of such action plan;
- Initiating the implementation phase by engaging the relevant stakeholders and determining ways of working (e.g., working groups, committees, frequency of meetings, actions log);
- Defining how the individuals responsible and accountable for the program will report to senior leadership on progress and risks, and developing templates and a methodology to enable such reporting (e.g., workstream owners could fill out dashboards every week/month outlining the status of actions planned, reasons for running behind schedule, specific risks and issues, and any needs for changing the plan); and

- Transitioning program implementation to program maintenance, monitoring and assurance.

CIPL has developed a methodology to support organizations in structuring and implementing data privacy management programs based on the elements of accountability—the CIPL Accountability Framework (see the figure below).[xviii] CIPL has also identified a number of organizations that apply this methodology to their own data privacy management programs and has listed real and concrete examples of how organizations implement accountability in data privacy.[xix] The LGPD requirements for privacy compliance and governance programs are mapped against the CIPL Accountability Framework in Appendix 1.

Key steps for consideration:

- Design a data privacy management program and an action plan for implementing it based on the identified risks.
- Identify easier tasks and implement them as soon as possible.
- Maintain and review the data privacy management program on an ongoing basis.

The CIPL Accountability Framework—– Universal Elements of Accountability

Priority 7. Define the legal bases for the organization's data processing activities

The LGPD requires organizations to only process personal data if they can rely on one of the legal bases for processing outlined therein (Article 7):

- Consent;
- Legal obligation;
- The exercise of public policies, its public function, or the pursuit of the public interest by the public administration;
- The undertaking of studies by research organizations;

- The performance of a contract or preliminary activities related to the contract;
- The exercise of rights under legal proceedings;
- The protection of the vital interests and physical safety of data subjects or third parties;
- The protection of health by health professionals;
- Legitimate interests of controllers or third parties; and
- The protection of credit.

In addition, the LGPD provides that organizations can only process sensitive personal data if they obtain the data subject's consent, in a prominent manner, for a specific purpose. Absent the data subject's consent for using sensitive data, organizations can rely on all of the other legal bases listed under Article 7, except contractual necessity, legitimate interests and the protection of credit (Article 11). In addition, organizations can also process personal data to prevent fraud and to ensure the safety of data subjects in the context of identification and authentication of registrations in electronic systems (Article 11, II, g).

The LGPD, like other data protection laws such as the GDPR, does not establish a hierarchy between the different legal bases (except in relation to the processing of sensitive personal data, as seen above). This means that consent is not elevated as a preferred option above the performance of a contract, legitimate interests or vital interests. In fact, there are many contexts and circumstances in which obtaining consent can be impractical, impossible, ineffective or not meaningful, and could lead to consent fatigue:

- Where there is no direct interaction with individuals;
- Where the data use is common, trivial and imposes no real privacy risk;
- Where large and repeated volumes of data are processed; and
- Where obtaining consent would be counterproductive such as where data is processed to prevent fraud or crime, or ensure information and system security.

Organizations should first define the individuals or teams responsible for determining the legal bases for processing. They must have a full understanding of the specific LGPD requirements for each legal basis. In addition, they may be responsible for undertaking LIAs—the balancing test required to determine if legitimate interests is the most appropriate legal basis for certain processing activities.

The responsible individuals or teams should define the legal basis for processing that is most appropriate to their specific data processing activity and type of personal data. When organizations undertake multiple processing activities, they should assess what legal basis they rely upon in each specific case. For instance, organizations may rely on the performance of a contract to process employee data for purposes of payroll, and on the protection of vital interests and physical safety of their employees when measuring their employee's body temperature onsite for the purposes of preventing the spread of COVID-19.

Keeping evidence of this decision-making process is also important for accountability purposes, as organizations need to be able to demonstrate compliance. In fact, the LGPD also requires organizations to keep records of data processing activities, especially when based on their legitimate interests (Article 37).

Organizations should also make considerations as to the processes to be put in place and/or adapted in connection with defining the legal bases for processing personal data:

- The individuals or teams responsible for defining the legal bases for processing should be able to review their decisions in case there are any new processing activities or updates to existing processing activities.
- Additional processes should be put in place in connection with specific legal bases for processing, such as:
    - Evidencing consent (Article 8, paragraph 2);
    - Allowing data subjects to withdraw their consent at any time (Article 8, paragraph 5);
    - Undertaking LIAs (Article 10, paragraph 3);
    - Ensuring that the organization only processes personal data that is strictly necessary in case it relies on legitimate interests (Article 10, paragraph 1); and
    - Adopting additional transparency measures connected to legitimate interests (Article 10, paragraph 2).
- Organizations should also consider combining related processes (legal bases, data mapping, records for processing activities, PIAs, LIAs, etc.). This would enable them to make informed decisions on whether they should stop collecting, delete or anonymize personal data that they no longer need for the purposes of the processing activities, in line with the principle of necessity (Article 6, III; and Article 12).

Key steps for consideration:

- Identify the individuals or team that will be responsible for determining the legal bases for processing—they should define the legal bases the organization relies upon as a priority.
- Consider what processes should be put in place and/or adapted for ongoing maintenance of the legal bases for processing activities.

Priority 8. Define technical and organizational measures for effective data security and internal reporting and management of security incidents

Technical and administrative data security measures

Data security is one of the principles of the LGPD (Article 6, VII and Article 46), requiring organizations to use technical and administrative measures to protect personal data from unauthorized access, and from accidental or unlawful processing, destruction, loss, modification, communication or sharing of data. In the context of this principle, organizations must:

- Adopt data security measures throughout the entire product development lifecycle (Article 46, paragraph 2);
- Adopt data security measures in all data processing systems (Article 49);
- Ensure data security even after the end of data processing activities (Article 47); and
- Address data security in DPIAs (Article 38, sole paragraph).

Organizations must implement technical and administrative data security measures taking into account the risks of data processing operations to individuals and to the organization (see Priority 5). Many global organizations dedicate specific work streams to implementing data security measures in their data privacy management programs. The teams responsible for such programs have to work hand in hand with the chief information officer as well as the information security and system/data architecture teams to determine the changes needed according to the risks of processing to individuals, define the time for implementing them, and update policies and processes accordingly.

Security incidents and personal data breaches

In addition to data security, the LGPD also has specific requirements concerning security incidents, including breaches of personal data:

- Privacy and data governance compliance programs must address response and remediation plans for security incidents (Article 50, paragraph 2, I, g);
- Controllers must notify the ANPD and data subjects of security incidents that may result in relevant risk or harm to individuals (Article 48); and
- Controllers may have to implement mitigation measures determined by the ANPD (Article 48, paragraph 2).

A lack of appropriate data security measures increases the risk of security incidents and data breaches. **Data breaches may have a significant impact on the organization from various perspectives**:

- Regulatory perspective: the ANPD may issue fines and the controller may be considered liable;
- Judicial perspective: individuals can file lawsuits against controllers and operators, and also some public institutions can file collective civil actions against such processing agents; and
- Reputational perspective: data breaches attract more attention in the media.

Even the most mature organizations are likely to experience data breaches. Hence, organizations should clearly define a methodology to prevent, identify, assess, manage/contain, mitigate and notify about breaches. They should also set up an ad hoc crisis management process and test the process through table-top exercises with senior management and other relevant stakeholders within the organization.

When devising a security incident and data breach response and mitigation process, organizations should consider implementing the steps below:

- Appoint a specific team—with relevant stakeholders from functions such as information security, legal, communications and the DPO—to manage the incidents and define whether this team should be on call 24/7;
- Define a risk assessment methodology to measure the risk of harm of security incidents, take the appropriate mitigation measures and identify whether the incident qualifies as a "reportable security incident" under the LGPD, considering the LGPD requirement to notify the ANPD "within a reasonable timeframe" that may be further specified by the ANPD itself (Article 48, paragraph 2);
- Provide special training to all staff to ensure that they are able to identify when a security incident has occurred and know where and how they should report it;

- Align with operators and contractors on how to report and provide information about security incidents to controllers in a timely manner;
- Develop tools, or adopt off-the-shelf tools, to support the management of breaches—such as the ones provided by OneTrust,[xx] TrustArc[xxi] and others[xxii]; and
- Ensure that the process addresses a review of the root cause of the security incident and the implementation of measures to mitigate an ongoing attack or prevent similar incidents in the future (e.g. additional training, system changes, specific training).

Key steps for consideration:

- Work with the information security and systems/data architecture teams to determine the changes needed to implement appropriate data security measures.
- Establish a process for internal reporting and managing of security incidents and personal data breaches and notifying the ANPD if necessary.

Priority 9. Identify all third parties with which the organization shares personal data and establish a third party management process

The LGPD sets out specific obligations for organizations when they qualify as controllers and/or operators (see Priority 4), including that controllers can verify whether operators are acting in accordance with data protection rules (Article 39). In addition, the LGPD establishes the following related principles:

- The principle of prevention, which establishes that organizations should adopt measures to prevent harms resulting from data processing (Article 6, VIII); and
- The principle of accountability, which establishes that organizations should be able to demonstrate that they have adopted efficient measures to comply with data protection rules (Article 6, X).

Third parties often represent an area of high risk from a data protection perspective. **Organizations must have a clear understanding of the organizations with which they share personal data and which process personal data on their behalf**, as well as understand their roles as controllers and/or operators in this context. They should **manage the relationship with operators and third parties to ensure that personal data is protected across the entire ecosystem**. As a matter of good practice, controllers should only choose operators that have appropriate data protection and security measures in place and that are willing to cooperate on data protection matters.

There are many ways organizations can manage their relationship with operators and third parties in order to address data protection risks. The measures adopted will vary depending on the context of the operators' and third parties' data processing activities, the types of data processed and the extent to which they engage with such third parties. Examples of third party management activities include:

- Implementing specific policies and procedures for third party management;
- Assessing and reassessing the risks of third parties such as through due diligence and assurance—which, in particular, can also be helpful to determine what mechanisms should be put in place to mitigate such risks (e.g., updating contractual clauses, putting in place new contracts, adopting security measures, auditing operators on a regular basis);

- Negotiating and managing contracts (e.g., implementing data processing agreements, updating data protection and security clauses in existing contracts);
- Undertaking audits and reviews on third parties' processing of personal data; and
- Engaging with third parties throughout the relationship and responding to any data protection queries they may have.

Key steps for consideration:

- Identify the third parties that process personal data on the organization's behalf, and determine whether it processes personal data on behalf of another organization.
- Assess and adopt third party management mechanisms, including due diligence and entering into data processing agreements.

Priority 10. Identify the organization's cross-border data flows (inbound and outbound) and put in place appropriate data transfer mechanisms and safeguards

The LGPD enables organizations to engage in international transfers of personal data to adequate third countries and international organizations (Article 33, I). In the absence of adequacy decisions by the ANPD, **organizations can engage in such transfers if they implement any of the following safety mechanisms**:[xxiii]

- Adoption of contractual clauses that are specific to the international transfer being made (Article 33, II, a);
- Adoption of standard contractual clauses (Article 33, II, b);
- Adoption of global corporate norms (Article 33, II, c);[xxiv]
- Adherence to seals, certifications and codes of conduct (Article 33, II, d);
- Obtaining individuals' consent specifically for the international transfer (Article 33, VIII); and
- Reliance on a specific legal basis (the need to protect the life and physical safety of individuals, compliance with a legal obligation, need to transfer data for contractual necessity, and need to transfer data in the context of a judicial proceeding) (Article 33, IX).

The LGPD also allows international transfers of personal data when:

- Necessary for judicial cooperation between public organizations (Article 33, III);
- Necessary for the protection of the life or physical safety of individuals (Article 33, IV);
- The ANPD authorizes the transfer (Article 33, V);
- They result in international cooperation agreements (Article 33, VI); and
- Necessary for the execution of public policies and services (Article 33, VII).

Some international transfer mechanisms depend on the establishment of the ANPD, as the ANPD must further establish and specify these transfer mechanisms. These include standard contractual clauses, contractual clauses specific to international transfer, global corporate norms and seals, certifications and codes of conduct. If the ANPD establishes further rules for these mechanisms, or

reviews the mechanisms already put in place by certain organizations, organizations will need to adapt accordingly.

International transfers of personal data are essential for businesses that operate across borders, and these transfers are more and more common in the digital economy. **In order to determine the most appropriate mechanism for their specific data transfers, organizations should first identify such transfers and their purpose**. For instance, an organization may rely on contractual clauses specific to a one-off transfer of personal data to a third country, while other organizations may rely on global corporate norms if they systematically transfer personal data to other entities of the same corporate group that are located in a third country. **This exercise can be done in the context of the data mapping** (see Priority 3).

Some organizations are looking at international examples of similar mechanisms to be leveraged for the purpose of LGPD compliance, such as the European Commission's approved standard contractual clauses,[xxv] and the European Data Protection Board (EDPB)'s guidance on BCR[xxvi]. In addition, some certification mechanisms have already been created in the context of the LGPD,[xxvii] and **many organizations rely on international certification schemes as part of their wider accountability programs**—such as the certifications provided by the International Organization for Standardization (ISO), the APEC Cross-Border Privacy Rules (CBPR) and the National Institute of Standards and Technology (NIST). In fact, **these certification schemes allow organizations to apply a consistent approach towards data privacy both internationally and domestically, and are key to providing some degree of legal certainty to these approaches in particular in the absence of further ANPD guidance**.

Key steps for consideration:

- Identify whether the organization transfers personal data to third countries, for what purposes and in what capacity (as controllers and/or operators).
- Assess and implement the transfer mechanisms that are most appropriate for the organization.

Priority 11. Build effective processes for transparency and data subject rights

The LGPD gives individuals the right to obtain information about specified aspects of data processing and about their data protection rights. Individuals must be able to easily access information, and such information must be clear, adequate and comprehensive (Article 9). In addition, individuals have the rights to obtain specific information about:

- Data sharing between public and private organizations (Article 18, VII);
- The option of not providing consent and the consequences of this decision (Article 18, VIII); and
- The rationale behind decisions that are based solely on automated processing of personal data (Article 20, paragraph 1).

Controllers need to have a process in place to ensure privacy notices are kept up to date and that all versions of privacy notices that have been provided to individuals are appropriately stored and can be referenced if needed. It is important that information is provided appropriately, otherwise there may be consequences such as consent being invalid (Article 9, paragraph 1). **Controllers should**

therefore consider whether to also use resources other than formal privacy notices to relay key messages to individuals, such as privacy portals, dashboards, videos, FAQs, animations, icons, and dedicated privacy centers updated on an ongoing basis.

The LGPD also provides individuals with other data protection rights. Individuals must be able to exercise these rights with controllers free of charge (Article 18, paragraphs 3 and 5). They are the following:

- Confirmation of processing of their personal data and access to such data, immediately and in simplified format or in a comprehensive manner within 15 days of the request, provided by electronic or physical means as chosen by the individual (Article 19);
- Correction (Article 18, III);
- Anonymization, blocking the use of personal data, or deletion of personal data that is unnecessary or processed in violation of the LGPD (Article 18, IV);
- Portability (which still depends on ANPD regulation—Article 18, V);
- Deletion of data that is processed based on consent, with a few exceptions outlined in Article 16;
- Withdrawal of consent (Article 18, IX);
- Objection to processing of personal data that is processed based on a legal basis other than consent, as long as the interest of the data subjects overrides the interest of the data controller (Article 18, Paragraph 2); and
- Review of decisions that affect the interests of individuals that are based solely on automated processing of personal data (Article 20).

The LGPD requires controllers to adopt measures to fulfill data protection requests "immediately." If the controller is not involved in the processing activities at issue in the request, it should immediately communicate that fact to the requestor and, to the extent possible, specify the correct controller or operator (Article 18, paragraph 4). These requirements indicate that **the LGPD allows individuals to have their data subject rights requests met within a reasonable timeframe**. This timeframe will vary depending on the scope of and nature of the request, the size of the organization, how many systems and databases process personal data and whether they are interoperable, and the specific data protection right being exercised (deleting data across various systems may take longer than informing individuals what data the organization holds). **There is one exception—the LGPD establishes a clear timeframe of 15 days for organizations to fully respond to access requests, even if a shorter-form response is to be provided immediately** (Article 19).

Experiences in other countries have shown that comprehensive data protection laws lead to a surge in data subject requests—see, for instance, the figures that can be found in annual reports of European data protection authorities.[xxviii] It is, therefore, important that controllers establish effective processes to respond to such requests. **Brainstorming different case scenarios where data subjects exercise their rights may be helpful for controllers to gather insights and prioritize**. For instance, they may decide between adopting manual processes (which may be more burdensome but are operationally faster), developing automated solutions (which may be costly and take longer to implement) or outsourcing off-the-shelf data subject rights management tools such as the ones provided by OneTrust,[xxix] TrustArc[xxx] and others.[xxxi]

When developing processes to handle data subject rights requests, controllers should take some key elements into account:[xxxii]

- The individuals and teams that will be involved in the process;
- How to verify a requestor's identity;
- What the most appropriate channel and/or tool would be to enable individuals to make a request (e.g., online web forms and dedicated email addresses);
- How to identify when a request is coming from unusual channels (e.g., individuals calling a customer center number);
- How to identify the scope of the request;
- Whether to put in place standard responses to be used by the individuals or teams responsible for responding to requests;
- Whether the organization intends to anonymize personal data after a deletion request;
- Whether cooperation is needed from operators; and
- Whether there are any technological or infrastructure challenges that need to be resolved.

In addition, organizations must involve the DPO in this process and in communications with data subjects (Article 41, paragraph 2, I and III), and immediately notify other controllers and operators involved in the processing operations when such a request is made (Article 18, paragraph 6).

Key steps for consideration:

- Prepare privacy notices and other relevant resources to provide easily accessible information to individuals about the organization's data processing.
- Map the various case scenarios for data subject rights requests and assess the organization's response time to requests to develop the relevant processes.
- Develop processes to respond to such requests.

Priority 12. Train employees on LGPD requirements and create an awareness-raising program

The LGPD does not have an explicit requirement for organizations to provide training to employees on data protection matters. However, **training and awareness are key components of embedding data privacy and accountability in the culture of organizations, and are also key components of data privacy management programs**. In fact, the LGPD establishes that organizations must be able to demonstrate that they are committed to adopting processes and internal policies that ensure compliance with the rules and good practice set out in their data privacy management programs (Article 50, paragraph 2, I, a).

Examples of training and awareness activities implemented by organizations include:[xxxiii]

- General data privacy training provided to all employees about the data privacy management program and data privacy fundamentals—such as privacy principles, basic obligations, data protection rights and how to identify and report a data breach;

- Targeted and role-specific training to teams such as legal, engineering, product development, data analysts, human resources, marketing, and information security;
- E-learning platforms, videos and other interactive and innovative elements;
- Data privacy-dedicated events to discuss privacy topics and developing privacy solutions; and
- Regular, concise, visual and practical communications and reminders to all employees to address specific topics such as privacy "do's and don'ts," FAQs, privacy by design, DPIAs and escalating data breaches.

Organizations should plan the most appropriate training and awareness activities in the early stages of establishing their data privacy management program, and should update them on an ongoing basis. They should define the number, comprehensiveness and type of training and awareness activities based on their number of employees, other existing training and awareness programs and the internal culture and structure of the organization. Larger organizations should implement a more strategic, comprehensive and organization-wide data privacy communication and awareness plan, which can be global, local or both. They should formally plan, budget and set up campaigns and communication strategies that are tailored to their business and culture.

Key steps for consideration:

- Implement ongoing training for all existing employees, contractors and new-joiners.
- Plan training and communications activities both in the beginning of the organization's data privacy management program and on an ongoing basis.

III. CONCLUSION

The LGPD has changed the Brazilian data protection regulatory and compliance landscape, and has established many new requirements that public and private organizations will need to implement. For many organizations, this is the first time they will have to deal with comprehensive data privacy compliance, and there are many open requirements in the LGPD that still need to be further specified, in particular by the ANPD. However, data privacy has been a topic in many jurisdictions around the world for decades, and to the extent possible, these organizations should look at and draw from international experience when handling similar LGPD requirements.

This paper brings the Brazilian community a set of areas that organizations should prioritize for LGPD compliance, with practical steps based on accountability that global organizations have implemented to comply with various data privacy laws around the globe. Organizations should adapt these steps to their own context, taking into account their size, types of processing activities and personal data processed, their internal corporate culture and business sector practices.

If you would like to discuss any of the comments in this paper or require additional information, please contact Bojana Bellamy, bbellamy@huntonAK.com; Markus Heyder, mheyder@huntonAK.com; Nathalie Laneret, nlaneret@huntonAK.com; Giovanna Carloni, gcarloni@huntonAK.com, Laura Schertel Mendes, lsm@lauraschertel.com.br; or Danilo Doneda, danilo@doneda.net.

Appendix 1. LGPD compliance elements mapped to the CIPL Accountability Framework

Leadership and Oversight	• Data protection officer • Mandatory LGPD governance program integrated into the organization's general governance structure	
Risk Assessment	• Impact assessment report as requested by the ANPD • Risk assessment of data incidents	• Risk-based approach to development of codes of conduct • Systemic assessment of impact on, and risk to, privacy as part of LGPD governance program
Policies and Procedures	• Legal bases and fair processing • Anonymization procedures • Retention and deletion • Review of automated decisions • Data transfer mechanisms • Internal technical and organisational measures to comply with LGPD	• Security measures for operators • Further technical measures required by the ANPD • Privacy by design • Vendor/operator contracts • Procedures for response to individual rights • Codes of conduct
Transparency	• Access to information about data processing • Special measures for transparency when processing is based on legitimate interests • Special notices for children and the elderly	• Goal of the LGPD governance program of building trust with individuals though transparency and participation mechanisms • Publication of codes of conduct
Training and Awareness	• Ability to demonstrate commitment to adopt internal procedures and policies resulting from the LGPD governance program—training implied	
Monitoring and Verification	• Evidencing consent • Verifying parental consent • Legitimate interest impact assessment • Internal records of processing	• Internal and external compliance monitoring for the LGPD governance program • Assessment of effectiveness of the LGPD governance program
Response and Enforcement	• Data incident response plans and remediation, breach notification • Audit for discrimination resulting from automated decision-making • Operator liability	• Demonstrating effectiveness of the LGPD governance program • Sanctions for non-compliance • Mandatory public consultation for ANPD guidance and requirements • Public hearings organised by the National Council

Appendix 2. LGPD obligations for controllers and operators

Note: the obligations listed in the table below refer to the LGPD provisions where the terms "controller" and "operator" are expressly mentioned or implied, and do not include obligations addressed solely at public organizations (Chapter IV). As mentioned in Priority 4 of this paper, even though many of the obligations do not directly apply to operators, they will need to make themselves available to support controllers in fulfilling such obligations.

Obligation	LGPD reference	Applies to controllers	Applies to operators
Define the legal bases for processing personal data	Article 7	✓ (implied)	X
Provide information to data subjects about personal data processing activities	Article 8, paragraph 6 Article 9 Article 14, paragraph 2	✓	X
Ensure the transparency of processing personal data based on legitimate interests	Article 10, paragraph 2	✓	X
Provide LIAs to the ANPD if required	Article 10, paragraph 3	✓	X
Verify the identity of legal guardians providing consent on behalf of children	Article 14, paragraph 5	✓	X
Delete personal data at the end of the data processing activity	Article 16	✓ (implied)	✓ (implied)
Receive and respond to data subject rights requests and inform other controllers and operators of actions needed to fulfill such requests	Article 18 Article 18, paragraph 6	✓	X
Put in place appropriate data transfer mechanisms and safeguards	Article 33, II	✓	X
Keep records of personal data processing activities	Article 37	✓	✓
Provide DPIAs to the ANPD if required	Article 38	✓	X
Process personal data as per the instructions of controllers	Article 39	X	✓
Appoint a DPO	Article 41	✓	X
Provide compensation for harms and damages related to the data processing activities	Article 42	✓	✓
Adopt technical and organizational measures to ensure the security of personal data	Article 46 Article 47	✓	✓
Notify the ANPD and data subjects about security incidents and adopt any measures required by the ANPD	Article 48 Article 48, paragraph 2	✓	X
Implement a data privacy management program	Article 50 Article 50, paragraph 2	✓	✓

[i] This paper was drafted by the Centre for Information Policy Leadership (CIPL) in collaboration with the *Centro de Direito, Internet e Sociedade* of the *Instituto Brasiliense de Direito Público* (Cedis/IDP). CIPL is a global privacy and security think tank based in Washington, DC, Brussels and London. CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for privacy and responsible use of data to enable the modern information age. Cedis/IDP is an institution focused on promoting research and debates on the implementation of new laws and regulations that impact the information society such as relating to privacy and data protection, competition and innovation, and internet governance. Cedis/IDP organizes events, workshops, research groups and partnerships with Brazilian and global organizations.

[ii] To understand more about the Project "Effective Implementation and Regulation Under the New Brazilian Data Protection Law (LGPD)," see <https://www.informationpolicycentre.com/brazilian-data-protection-implementation-and-effective-regulation.html>.

[iii] Available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (official publication in Portuguese).

[iv] This paper applies to organizations who fall within the scope of the LGPD according to Articles 3 and 4.

[v] See the CIPL paper The Role of the Brazilian Data Protection Authority (ANPD) under Brazil's New Data Protection Law (LGPD), available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[en]_cipl-idp_paper_on_the_role_of_the_anpd_under_the_lgpd__04.16.2020__3_.pdf>.

[vi] As of the date of publication of this paper, the ANPD has not assumed its operations. However, on August 27, 2020, the Brazilian President published in the Official Journal the Decree 10.474/2020 approving the ANPD's regulatory structure and establishing its roles. This Decree will be applicable after the President-Director of the ANPD is officially appointed through publication in the Official Journal. Available at <https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226>.

[vii] CIPL has worked extensively on the concept of organizational accountability and has published a series of papers outlining the elements of accountability and how organizations can operationalize accountability, including "What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework," available at <https://www.informationpolicycentre.com/organizational-accountability.html>; "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society", available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf>; and "Incentivizing Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf>. Other CIPL papers on accountability are also available on CIPL's website at <https://www.informationpolicycentre.com/cipl-white-papers.html>.

[viii] From Privacy to Profit: Achieving Positive Returns on Privacy Investments—Cisco Data Privacy Benchmark Study 2020. Published in January 2020. Available at <https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2047256&utm_source=newsroom.cisco.com&utm_campaign=Release_2047256&utm_medium=RSS>.

[ix] On 16 January 2019, the Special Unit of Data Protection and Artificial Intelligence of the Public Prosecution's Office of Distrito Federal made an agreement with Netshoes in the context of an investigation on data breaches of almost two million individuals, which occurred in 2017 and 2018. According to the agreement, the company committed to (1) implementing additional measures to its data protection program, including to comply with the LGPD; (2) notifying individuals about the breaches and raising awareness of data security risks to individuals; (3) raising awareness of good privacy and data protection practice to other organisations such as through participating in discussions and relevant events; and (4) paying a fine of R$500,000 for collective moral/non-material damages. The Agreement makes reference to a series of legal provisions concerning the protection of personal data within the Federal Constitution, the Brazilian Civil Rights Framework for the Internet—Marco Civil da Internet, the consumer code as well as the LGPD, noting that the LGPD was not yet applicable by then. If Netshoes fails to comply with the agreement, the Public Prosecution's Office will initiate

a public civil action against in the value of R$10 million. Available at <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10570-mpdft-e-netshoes-firmam-acordo-para-pagamento-de-danos-morais-coletivos-apos-vazamento-de-dados>.

[x] On 18 December 2018, the Public Prosecution's Office of Distrito Federal settled a public civil action which had been initiated by its Special Unit of Data Protection and Artificial Intelligence against Banco Inter for the breach of banking-related personal data of almost 19,000 individuals. According to the settlement, the bank had to pay R$1,5 million, part of which will be destined to public institutions that work on fighting cybercrimes. The Public Prosecutor's Office had accused the bank of violating the consumer code, which establishes that service providers are liable for damages caused to consumers resulting from faulty services, including when the services do not provide the level of security that is expected by consumers (Article 14 of the consumer code). Available at <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2018/10524-2018-12-19-10-27-31>.

[xi] On 5 December 5, 2018, the consumer authority of Minas Gerais state (Procon-MG) issued a R$7 million fine to a drug store (Drogaria Araújo) for requiring consumers to provide their ID number in order to obtain discounts on items being purchased. The authority alleged violations of the consumer code concerning the provision of clear information to consumers, including about the risks to data security; as well as the provision that requires companies to communicate to consumers, in writing, when they are going to be registered within their systems. The authority has also questioned the drug store's capabilities for ensuring the security of such personal data, and mentioned possible data breaches. Available at <https://www.mpmg.mp.br/comunicacao/noticias/drogaria-araujo-devera-pagar-multa-de-r-7-milhoes-por-capturar-cpf-dos-consumidores.htm>.

[xii] See endnote n. vi.

[xiii] Privacy Impact Assessment (PIA), available at <https://www.cnil.fr/en/privacy-impact-assessment-pia>.

[xiv] Data protection impact assessments, available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>.

[xv] NIST Privacy Framework, available at <https://www.nist.gov/privacy-framework>.

[xvi] OneTrust PIA & DPIA Automation solution, available at <https://www.onetrust.com/products/assessment-automation/>.

[xvii] TrustArc DPIA & PIA solution, available at <https://trustarc.com/gdpr-dpia-pia-solutions/>.

[xviii] See endnote n. vi.

[xix] See endnote n. vi.

[xx] OneTrust Incident and Breach Management tool, available at <https://www.onetrust.com/incident-and-breach/>.

[xxi] TrustArc Incident Response and Breach Management tool, available at <https://trustarc.com/blog/incident-response-breach/>.

[xxii] The IAPP maintains a list of tech vendors who provide privacy solutions, including to managing incident responses and data subject rights at <https://iapp.org/resources/article/privacy-tech-vendor-report/>. Other tools used by organizations in Brazil include: Privally <https://privally.global/>; Pontus Vision <https://www.pontusvision.com/>; Securiti.AI <https://securiti.ai/>; MD2Net <http://www.md2net.com.br/solucoes/lgpd-suite.php>; Axon Data Governance <https://www.informatica.com/br/products/data-quality/axon-data-governance.html>.

[xxiii] A couple of other international data transfers options established by the LGPD are also specifically relevant to public organizations—when transfers are needed for international cooperation between public intelligence, investigation and enforcement bodies, and for the execution of public policies.

[xxiv] Note that the LGPD uses the term "global corporate norms" for what is referred to in other data protection laws such as the GDPR as "binding corporate rules."

[xxv] European Commission's standard contractual clauses, available at <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en>.

[xxvi] A series of guidance documents by the EDPB on BCR can be found at <https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en>.

[xxvii] See for instance the certifications Abemd-Bureau Veritas <https://abemd.org.br/LGPD/Programa_Abemd_LTSA_BV_LGPD.pdf>, Abradi-Bureau Veritas <https://abradi.com.br/projetos/abradi-lanca-certificacao-para-lgpd-e-cartilha-de-protecao-de-dados-pessoais/>.

[xxviii] For instance, the Irish Data Protection Commissioner noted in its 2019 Annual Report that it has received 7,215 complaints since the GDPR came into effect, and that 6,069 valid data security breaches were notified representing a 71% increase on the total number of valid data security breaches (3,542) recorded in 2018. Annual Report, 1 January—31 December 2019. Available at <https://www.dataprotection.ie/en/data-protection-commission-publishes-2019-annual-report>.

[xxix] OneTrust Consumer & Data Subject Rights Management tool, available at <https://www.onetrust.com/products/data-subject-access-requests-portal/>.

[xxx] TrustArc Individual Rights Manager tool, available at <https://trustarc.com/individual-rights-manager/>.

[xxxi] See endnote n. xvi.

[xxxii] See the CIPL White Paper on Data Subject Rights under the GDPR in a Global Data Driven and Connected World, available at <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_data_subject_rights_under_the_gdpr_in_a_global_data_driven_and_connected_world__8_july_2020_.pdf>.

[xxxiii] See more examples in the CIPL Accountability Mapping Report—see endnote n. vi.