Paper 3 of the Joint Project on Effective LGPD

The role of the Data Protection Officer ("Encarregado") under the Brazilian General Data Protection Law (LGPD)

Centre for Information Policy Leadership (CIPL)

and

Centro de Direito, Internet e Sociedade of Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (CEDIS-IDP)

27 September 2021

This is the third paper of the special Joint-Project "Effective Implementation and Regulation Under the New Brazilian Data Protection Law (LGPD)" by CIPL and CEDIS/IDP.[1] 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/effective-lgpd.html>.

CONTENTS

[1] 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 Brasileiro de Ensino, Desenvolvimento e Pesquisa* (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 those 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.

SUMMARY OF RECOMMENDATIONS FOR THE ANPD FOR ITS COMPLEMENTARY RULES CONCERNING THE ROLE OF THE DPO

- Adopt an approach that is flexible, pragmatic, instructive and risk- and outcomes-based, rather than prescriptive or primarily punitive.
- Reinforce that the role of the DPO under the LGPD is different compared to this role under the GDPR, in particular with regards to the DPO's independence and conflicts of interest requirements.
- Acknowledge the importance of the DPO for organizational accountability.
- Acknowledge that the DPO is not a one-size-fits-all role and allow organizations the flexibility to define the DPO role as appropriate to their business and data processing activities (as long as it complies with the LGPD rules).
- Propose a set of criteria for organizations to consider when defining their needs in relation to the role of the DPO and examples of how they can establish this role internally and externally).
- Consider organizations having gone beyond the LGPD's and ANPD's DPO requirements as a mitigation factor in enforcement cases.
- Consider establishing a specific department within the ANPD dedicated to engaging with DPOs.
- Acknowledge that the DPO need not be involved in all data protection matters and leave it to organizations to define appropriate criteria for DPO involvement.
- Encourage organizations to adopt a risk-based approach towards the role of the DPO so that he/she/they are involved primarily in higher-risk and strategic matters.
- Provide flexibility for organizations to define their DPO's role in interacting with the public and the ANPD as appropriate to their business.
- Do not mandate additional tasks for the DPO that go beyond the core DPO tasks established by the LGPD—recommend and provide examples of additional tasks instead.
- Exempt organizations from the DPO requirement if their processing activities are low-risk.
- Encourage operators to appoint a DPO rather than making it mandatory in all cases.
- Allow a department within the organisation to fulfill the role of the DPO if appropriate.
- Allow organizations to appoint external DPOs if appropriate.
- Clarify that DPOs are not personally liable for the organizations' misconduct and non-compliance with the LGPD.
- Allow organizations to publish the contact details of the DPO office rather than the personal contact details of the individual fulfilling the role of the DPO to preserve his/her/their safety.

**The role of the Data Protection Officer ("Encarregado")
under the Brazilian General Data Protection Law (LGPD)**

1. INTRODUCTION—THE LGPD DPO REQUIREMENTS AND THE GOALS OF THIS PAPER

The Data Protection Officer (DPO) is a key feature of organizational accountability. The DPO is responsible for overseeing the implementation of the data privacy management program (DPMP), translation of legal obligations into concrete actions, documentation of data processing activities and decisions, and the training of relevant staff as part of the DPMP. (see Section 2) The Brazilian data protection law (*Lei Geral de Proteção de Dados Pessoais*—LGPD)[2] has introduced for the first time the role of the DPO in Brazil, under the name "encarregado". The LGPD DPO rules apply to both public and private sector organizations that fall within the wide scope of the law and will be further regulated by the ANPD in the first semester of 2022 according to Ordinance No. 11/2021 of the ANPD, which establishes the regulatory agenda of the authority.[3]

The name "encarregado" means a person who "is in charge" of the organization's data processing activities. We understand that this includes, among other activities, the organization's DPMP, which organizations are required to put in place to comply with the provisions of the LGPD.[4] Notably, the LGPD requirements are less prescriptive than the DPO requirements in data protection laws of other jurisdictions—such as the EU General Data Protection Regulation (GDPR), the Privacy (Australian Government Agencies—Governance) APP Code 2017, and Colombia's Law 1581/2012 and Decree 1074.[5] For example, unlike the GDPR, the LGPD does not require DPOs to be independent and free from conflicts of interest.

The LGPD DPO provisions are as follows:

- **Article 5, VIII** defines the DPO as the person appointed by the controller and the operator to act as the main point of contact between the controller, individuals and the Brazilian data protection authority (*Autoridade Nacional de Proteção de Dados Pessoais*—ANPD);
- **Article 41** specifies that controllers must appoint a DPO (no mention is made to operators);
- **Article 41, paragraph 1** establishes that the identity and contact details of the DPO must be publicly disclosed, in a clear and objective manner, preferably in the controller's website;
- **Article 41, paragraph 2** establishes that the DPO is responsible for (i) receiving and acting upon individuals' as well as the ANPD's requests, (ii) providing advice and guidance to the organization on data protection and LGPD compliance, and (iii) following any further instructions determined by the controller or by complementary rules;
- **Article 41, paragraph 3** establishes that the ANPD may issue complementary rules concerning the role of the DPO, including any exemptions to appoint a DPO; and

[2] Available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm (official publication in Portuguese).
[3] This paper applies to organizations that fall within the scope of the LGPD according to Articles 3 and 4. It should be noted that public entities do not fit perfectly into all the indications in this paper, but they can use this work to the extent that is compatible with their activities.
[4] Article 50 of the LGPD.
[5] For a comparison of the DPO requirements in data protection laws around the globe, see IAPP's Data Protection Officer Requirements by Country, 9 April 2021, available at https://iapp.org/resources/article/data-protection-officer-requirements-by-country/.

- **Article 23, III** clarifies that public organizations must also appoint a DPO.

As explicitly provided for by the LGPD, the DPO has a dual role of:

i. Protecting individuals with regards to their right to data protection as well as other rights that may be impacted by the processing of personal data; and

ii. Advising the organization on legal, commercial and reputational risks relating to non-compliance with the LGPD requirements.

It is positive that the LGPD is flexible as opposed to prescriptive in relation to the role of the DPO. The level of prescriptiveness regarding the DPO attributes varies in data protection laws, and experience has shown that the more prescriptive the legal rules concerning the DPO are (such as the ones in the GDPR), the more challenging it may be for organizations to implement this role in a way that fits their structure and culture. As seen above, the ANPD is tasked with issuing complementary rules on the role of the DPO and has included these rules as one of the top priorities in its regulatory agenda for 2021-2022.[6] In doing so, the ANPD should find the balance between providing clarity to organizations where needed and avoiding being overly prescriptive—providing examples and case studies may help the ANPD reach this balance.

There are many instances, however, where Brazilian and international organizations will need clear guidance concerning the role of the DPO under the LGPD. Organizations face practical challenges on determining whether they are actually required to appoint (or would benefit from appointing) a DPO and how this role should be positioned within the organization. Examples include where the DPO should sit geographically and within the company's structure and what should be his/her/their reporting lines; whether large organizations can appoint existing DPOs under other jurisdictions to act as the LGPD DPO; or whether the DPO must be internal or could be external to the organization. For more unresolved questions, please refer to Section 3.

This Paper seeks to address these challenges from a practical point of view, drawing from the experience and best practices of mature multinational organizations already subject to the obligation to appoint a DPO under other data protection laws. The ultimate goals of this Paper are to support:

i. Organizations in understanding the importance of the role of the DPO under the LGPD and the relevant considerations when creating a DPO position for their organization; and

ii. The ANPD in effectively addressing organizations' concerns and challenges when drafting their complementary rules on the role of the DPO.

2. THE IMPORTANCE THE DPO FOR ORGANIZATIONAL ACCOUNTABILITY

Accountability is a key building block for effective data protection. It operationalizes legal obligations and behavioral goals into concrete data protection controls, policies, procedures, tools and actions within an organization. It also places responsibility on organizations to exercise judgment in carrying out contextual analyses to establish the level of risk created by their personal data processing activities and in applying relevant risk mitigation measures. Accountability is not set in stone but requires ongoing adaptation and an internal change management process to keep pace with evolving laws, regulations, technology, and business practices.

[6] Available at https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313 (official publication in Portuguese).

Accountability is a core principle under the LGPD.[7] 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 a comprehensive DPMP and (ii) are able to demonstrate the existence and effectiveness of such actions and controls internally and externally.

As already mentioned, **the DPO is a core element of organizational accountability**. This role is instrumental in enabling that privacy compliance and the DPMP are properly adapted to the privacy risk profile of the organization as well as the varying risks of processing activities. Consequently, it is important that the DPO is seen as having a strategic function within the organization. The DPO should be considered as a trusted business advisor and enabler of innovative data uses, ensuring that privacy considerations are brought up early in the planning and design phase of data processing operations.

Appointing a DPO is one of the first things that organizations should do when developing and implementing their DPMP.[8] The DPO should have a strategic role as a trusted advisor, working in partnership with the organization's leadership and liaising with the business on data privacy but, possibly, also more broadly on all data or digitally-related matters. This will depend, of course, on how the organization views this role as well as the size of the company and the importance of data and digital issues for its business. While it is possible to focus this role solely on operational tasks relating to data protection and LGPD compliance (e.g., managing data subject rights requests), leading accountable organizations leverage this role more broadly to be strategic from an accountability standpoint.[9] This strategic positioning of the DPO is even more relevant for organizations that have a data-driven business model.

Case study 1. DPO has helped raise awareness of the DPMP and gain client trust

Having a DPO in charge of the DPMP has enabled a large multinational organization headquartered in Brazil to raise awareness on the program internally. The DPO's role has enhanced employees' engagement in program activities as they feel that the program "has a face" and they know who to contact. It also allowed this organization to gain client trust, given that the DPO engages with clients to explain what measures the company is taking to become accountable in data privacy.

In fact, in recent years organizations have been increasingly recognizing the role of the DPO as a compliance enabler and an instrumental part of their accountability and data protection programs. Because the DPO's explicit role is to protect individuals with regards to the processing of personal data (which is a fundamental right in Brazil)[10], having a DPO helps to enhance individuals and customers' trust in the organization. It also raises the level of trustworthiness of organizations in the digital supply chain. Therefore, while only controllers may be required under the LGPD to appoint a DPO (see Section 1), processors should not overlook the importance of this role and may want to have their own DPO or a person with similar responsibilities. Controllers will be looking for assurance from their business

[7] See Article 6, X and Article 50 LGPD.
[8] See the CIPL and CEDIS-IDP paper on the Top Priorities for Public and Private Organizations to Effectively Implement the LGPD (in English and Portuguese).
[9] CIPL has developed the well-known CIPL Accountability Framework and has worked extensively on this concept, publishing 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; The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society; and Incentivizing Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability. Other CIPL papers on accountability are also available on CIPL's website.
[10] See the Brazilian Supreme Court Justice Rosa Weber's vote (in Portuguese) in the case of the Direct Unconstitutionality Actions (ADIs) 6387, 6388, 6389, 6390 e 6393.

partners that they are processing data in compliance with the LGPD and having a DPO may be a good way to provide such assurance.

Mature organizations subject to other legal regimes that require the designation of a DPO commonly establish a number of features for this role, which can be seen as best practice:

- Having a key role in the planning, implementing and overseeing the organization's DPMP—the DPO can be seen as a *chef d'orchestre*, working with and leveraging other relevant corporate functions in all the phases of the creation and maintenance of the DPMP;
- Reporting to senior leadership and/or the Board;
- Having deep knowledge of the organization and acting as its "collective conscience", taking into account that the DPO will make recommendations or decisions potentially impacting the business;
- Being involved in data strategy and data-related decisions—e.g., by having a seat at the table and access to top-level management, being consulted by the business in the early stages of product/service development, and ensuring appropriate attention to privacy by design;
- Acting and being accepted as a trusted business advisor and privacy champion (rather than being seen by the business as an internal "police officer"), based on clear internal communications to all relevant parts of the organization concerning the role and responsibilities of the DPO (e.g., through internal policies or a DPO Charter, as well as training and awareness);
- Being involved in business decisions concerning data privacy risks and responding to questions about data privacy risk assessments;
- Applying a risk-based approach to his/her/their activities through prioritizing areas of higher risk for individuals as well as for the organization;
- Maintaining a trusted relationship with the data protection authority (here the ANPD) and acting as its main interlocutor and contact point.

The ANPD has an important role in incentivizing organizational accountability, as higher levels of accountability will facilitate the realization of the LGPD's dual goals of data protection and economic growth. The ANPD should, therefore, affirmatively recognize and reward organizations that go above and beyond what the law requires to protect individuals' personal data. An example of treating the LGPD requirements as a floor rather than the ceiling would be when organizations define their DPO's responsibilities in a way that exceeds the LGPD requirements. Another example would be where those organizations that might be exempted from the DPO requirements by the upcoming complementary ANPD rules nevertheless decide to appoint a voluntary DPO on the basis that this will enable not only better compliance but also heighten the organization's general accountability and digital responsibility.

Recommendations for the ANPD for its complementary rules concerning the role of the DPO:

- Adopt an approach that is flexible, pragmatic, instructive and risk- and outcomes-based, rather than prescriptive or primarily punitive.
- Reinforce that the role of the DPO under the LGPD is different compared to this role under the GDPR, in particular with regards to the DPO's independence and conflicts of interest requirements.

- Acknowledge the importance of the DPO for organizational accountability.
- Acknowledge that the DPO is not a one-size-fits-all role and allow organizations the flexibility to define the DPO role as appropriate to their business and data processing activities (as long as it complies with the LGPD rules).
- Propose a set of criteria for organizations to consider when defining their needs in relation to the role of the DPO and examples of how they can establish this role internally and externally).
- Consider organizations having gone beyond the LGPD's and ANPD's DPO requirements as a mitigation factor in enforcement cases.

3. KEY CONSIDERATIONS FOR AN EFFECTIVE DPO

Regardless of whether the organization (controller or operator) has established the role of the DPO as focusing solely on the tasks prescribed by the LGPD or having a broader role, there are certain key considerations relevant to every organization when designating a DPO. These considerations vary depending on the organization's size, the risk of its data processing activities to individuals ("privacy risk profile"), internal governance structure, geographical scope, and business model.

At bottom, the effectiveness of the DPO depends on his/her/their ability to provide independent advice to the business including to shape its data processing decisions, as well as to engage directly with the ANPD. To facilitate this, organizations should consider the following key elements for the DPO role.

3.1. Expertise

First and foremost, **all DPOs must have expertise in the field of privacy and data protection** and may need expertise or knowledge on related fields such as relevant technology, cybersecurity and risk management. The DPO should understand relevant laws, regulations, regulatory guidance and other standards. Such understanding is key for the DPO to identify risks in the business and in product development, and to provide expert advice and guidance to the organization. It is also paramount that the DPO is able to communicate effectively at all levels of the organization, as well as with the public and the ANPD, when appropriate.

The DPO must have a good understanding of the business, as this will impact his/her/their ability to provide effective advice. While the DPO has a significant responsibility to represent the interests of the individuals whose data is being processed and ensuring compliance with the LGPD, he/she/they are also part of the business and an employee of the organization. Therefore, the DPO should also be able to understand and address any data protection questions and issues from a business perspective. This means, for example, that if the core of the business consists in commercializing artificial intelligence-based products, the potential DPO will need to demonstrate some degree of understanding of this technology, the impact it may have on individuals and how compliance with the LGPD requirements would be achieved.

Similar to the EU when the GDPR came into force, Brazil is currently experiencing a surge in demand for DPOs and other privacy professionals.[11] Even though the supply might be smaller than the demand

[11] "This year, it is Brazil's LGPD that is poised to trigger the most growth in the role of DPO. A recent study by IAPP estimated the newly implemented law will require 50,000 DPOs in Brazil alone." IAPP-FTI Consulting Privacy

in the initial years following LGPD applicability, there are a number of courses and certifications available for professionals specializing in the field of data protection. Most professionals that are currently specializing in this area come from legal backgrounds, but nothing prevents professionals from other backgrounds—such as engineering, information security, business management—to also specialize in data protection. Many organizations may also choose to invest in upskilling their current employees, who likely already have an understanding of the business, instead of hiring new employees for data protection roles and the DPO role.

3.2. Authority and reporting lines

It is also important that the DPO has sufficient authority in the organization so that his/her/their voice is heard and taken into account both by the organization's leadership and the business, when he/she/they provide strategic as well as day-to-day data protection advice. One way of ensuring sufficient authority is through establishing reporting lines (direct and/or indirect/dotted lines) from the DPO to those who have ultimate authority to make relevant decisions in the business, even if that does not mean the highest management level.[12] Therefore, each organization should decide the most appropriate reporting lines under their corporate structure (e.g., to a head of function/business, to senior leadership, to the Chief Privacy Officer, to the Board of Directors, to the CEO).

When deciding the most appropriate reporting lines, organizations should consider, for example, the following factors:

- The organizations' data processing activities, in particular those activities that present higher risk to individuals;
- Who are the key decision-makers within the business with regards to data processing activities; and
- Whether it is important that the DPO also has visibility with senior management and, perhaps, the Board of Directors.

For instance, smaller organizations may appoint a DPO under a management position, as long as this position provides him/her/them with sufficient access to, and influence on, its leadership and the teams who will be responsible for building products and services that impact individuals' data privacy. Larger

Case study 2. Internal senior and strategic DPO

A large Brazilian organization decided to appoint to the role of DPO under the LGPD a senior executive who has been working with the organization for 20 years. The organization decided to leverage internal existing resources because it is a large complex group of companies covering a diverse range of activities. This DPO is tasked with providing advice on data privacy matters that go beyond mere LGPD compliance—such as partnerships, mergers and acquisitions, and product development. The organization concluded that it would be essential that the DPO had deep knowledge about the business to be effective and strategic.

Case study 3. Change in the DPO's positioning in order to enhance its effectiveness

A multinational data-driven organization has changed the DPO's positioning and reporting lines from the policy team to the product team, as it has decided that being closer to product developers and engineers would enhance the DPO's impact on the level of compliance with the organization's data protection obligations.

Governance Report 2020, December 2020, available at https://iapp.org/resources/article/iapp-fti-consulting-privacy-governance-report-2020/.

[12] Note that reporting to the highest management level is a requirement of the GDPR, not of the LGPD. In the EU, this GDPR requirement has been subject of extensive debates and many organizations believe that it does not provide enough flexibility for them to structure the role of the DPO internally in the most effective manner.

organizations will likely have in place a more complex corporate governance structure, including several teams, functions and oversight bodies such as audit committees. In these cases, the DPO should have the ability to bring data protection matters to the organization's management/senior leadership, either directly or indirectly (e.g., through a Data Use Committee or escalation procedures).

Research by the International Association of Privacy Professionals (IAPP) found that the DPO is the privacy leader in 13% of the organizations that participated in their survey:

> *"DPOs tend to report into the organization's privacy leader (39%), general counsel (19%) or chief compliance officer (13%). The rest report directly into those higher up the corporate ladder, with 12% reporting to the board of directors, 8% reporting to an executive vice president and another 8% reporting directly to the CEO."*[13]

3.3. Positioning within the corporate structure

Organizations may position the DPO as an independent function or under an existing function within its organization. The positioning of the DPO will also depend on where the DPO's role would be most impactful, in light of the organizations' higher risk or most sensitive projects.[14]

Many organizations position the DPO under their Legal function. Other organizations position the DPO under Risk, Ethics, Compliance, Information Security, Product, Engineering, Audit or as a standalone function.

Both with respect to larger or smaller organizations, the DPO's positioning within the corporate structure is irrelevant as long as he/she/they have the ability to exercise his/her/their tasks under the LGPD appropriately and effectively.

Case study 4. DPO in the second line of defense

A multinational organization of the financial sector headquartered in Brazil has implemented the "three lines of defense" model for its data privacy governance structure, and has positioned the DPO in the second line, responsible for overseeing, monitoring and giving independent advice to the more operational role done by the first line.

3.4. Geographical positioning

The LGPD does not restrict an individual located outside of Brazil to be appointed as a DPO, as long as the DPO (including his/her/their team) is able to execute his/her/their tasks under the LGPD effectively (i.e., provide advice within the organization and act as the main point of contact with the public and the ANPD). Ideally, the DPO's team should be positioned in a time zone that would make meetings or calls with the ANPD and key decision-makers on data protection matters within Brazil possible (e.g., be available during the ANPD working hours). Notably, the accelerated digitization of businesses due to the COVID-19 pandemic has demonstrated that remote work can be effective and that territorial barriers are less important in a globalized world. Nonetheless, the DPO should be available to come to Brazil, if necessary and in case he/she/they is not located in the country.

---

[13] IAPP-FTI Consulting Privacy Governance Report 2020, December 2020, available at https://iapp.org/resources/article/iapp-fti-consulting-privacy-governance-report-2020/.

[14] Some organizations implement the "three lines of defence model" and position the DPO within this model (see case study 4). This model consists of functions that own and manage risks (first line), functions that oversee the first line's risk management activities and provide the policies, frameworks, tools, techniques and support to enable risk and compliance to be managed in the first line (second line), and functions that provide independent assurance such as internal audit (third line).

The organization will also need to consider any possible language barriers in case it decides to designate a non-Portuguese speaker as a DPO. Given that communications with individuals and the ANPD are among the core DPO tasks under the LGPD, the organization will need to ensure that measures are in place to close any language gaps in this case. This includes providing local support to the DPO and his/her/their team, adding Portuguese speakers to the DPO's team, having Portuguese-speakers involved in the internal processes to manage individual rights requests, and making available simultaneous translation during possible meetings with the ANPD.

The issue of geographical positioning of the DPO is particularly relevant for multinational organizations that are subject to data protection laws in other jurisdictions, which also require the appointment of a DPO. Such organizations may therefore leverage their already-appointed DPO, whose expertise and understanding of the organization's data protection measures and risks may be heightened by their knowledge of work under other jurisdictions, to fulfil the LGPD requirements, as long as due consideration has been given to the issues outlined above. They might also consider appointing DPOs to cover specific regions or languages to act as the main point of contact between the organization and individuals, as well as with the ANPD.

3.5. Involvement in data privacy matters

In order to act upon requests from individuals and the ANPD, as well as provide advice to the organization, the DPO must be appropriately involved in data protection matters. This includes being able to engage with and obtain information from all relevant functions and teams across the organization; being involved in key product reviews, risk assessments, and security incidents involving personal data; and being included in the discussions leading to relevant decisions concerning data processing. In parallel, functions within organizations should feel comfortable to openly share all relevant information and resources with the DPO necessary for the performance of his/her/their tasks, to work collaboratively with the DPO on data privacy matters, and to consider the DPO's feedback and advice.

The DPO's involvement in data privacy matters is also important to meet the expectations of regulators. Like other DPAs, the ANPD is likely going to expect that when interacting with an organization and its DPO, the organization will have consistent and synchronized positions and approaches to data privacy matters across all corporate functions. The DPO, being responsible for receiving and responding to the ANPD's requests, can act as the organization's main ANPD liaison, in particular on key data protection matters. For example, global DPAs have made clear that they expect DPOs to be involved in addressing the data privacy implications of any measures organizations have implemented as a result of the COVID-19 pandemic. Further, DPAs expect that the DPO will be their main point of contact rather than having different parts of an organization contacting them without the DPO's involvement.

However, there are data processing issues that do not rise to the level of requiring DPO involvement, such as minor security incidents or routine questions relating to data subject rights, which the DPO could delegate to his/her/their staff or to other teams within the organization. Depending on the organization, the DPO's involvement in data protection matters may have to be prioritized and focused on matters that are most relevant from a strategic perspective and that represent higher risks to individuals and the organization. Subject to complying with the LGPD, it should be left to organizations and their DPOs to decide when to escalate matters to the DPO. The specific escalation criteria could be included in a DPO charter or internal policies.

3.6. Skills and qualifications

There is no one-size-fits-all set of skills, qualifications and backgrounds for the DPO. Organizations adopt different approaches and DPOs, therefore, have a variety of backgrounds—ranging from legal and risk management, to engineering, audit, compliance and technology. It is important that the DPO has appropriately deep knowledge of the organization and of the sector(s) it belongs to, especially for highly regulated sectors or sectors relying on sensitive data uses. DPOs must have those skills that enable them to effectively discharge the duties of their role and to shape and drive robust data protection policies and measures across the entirety of their organizations.

Considering the DPO tasks under the LGPD (Section 4), it is important that the DPO have strong leadership, communication and analytical skills to navigate the complexities of the role and the organization they work for and be seen as an enabler of privacy and data protection within the organization. DPOs should be proactive in relation to their organization's privacy compliance, analyze and inform the organization about relevant external privacy developments, be able to identify and propose solutions to risks, identify problems and required changes and oversee their implementation.

In its Guidelines for Data Processing Agents and DPO, the ANPD has recognized that the DPO's professional qualifications shall be assessed by the controller, taking into account data protection and information security knowledge that meets the needs of the organization's operation.[15]

In summary, in addition to expert knowledge, essential DPO skills include:

- Leadership and business skills;
- Interpersonal skills and communication and teaching skills;
- Knowledge of the organization and of the business;
- Organizational and project management skills; and
- Analytical skills.

3.7. Resourcing

For DPOs to be able to effectively discharge their responsibilities, organizations must provide them with appropriate resources. Examples of resources include:

- Staffing resources—the DPO team;
- Adequate budget;
- Time (appropriate deadlines);
- Training for the DPO team (e.g., courses, workshops);
- Opportunities to attend conferences to exchange experiences and ideas with peers and learn about the latest trends;

[15] ANPD, Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, May 2021, available at https://urldefense.proofpoint.com/v2/url?u=https-3A__www.gov.br_anpd_pt-2Dbr_assuntos_noticias_2021-2D05-2D27-2Dguia-2Dagentes-2Dde-2Dtratamento-5Ffinal.pdf&d=DwMFAw&c=jxhwBfk-KSV6FFIot0PGng&r=jBvL0rmlt0xV9zh45T69YUWL4MGVIumoY2z1AbYxREU&m=LcqRVMGAcwwmNnvt7yEwUbN80kOwVijRgekoV2oItWI&s=v8JmwLsfGpa3hq376gIGckSsh2O2xKqIsqb8QhV6aK4&e=.

- Opportunities for the DPO team to obtain relevant professional certifications (e.g., data protection certifications);
- Access to external sources of relevant information on domestic and global data privacy, technological and business developments;
- Technology and tools relevant to their tasks (e.g., robust communication channels, data managing and mapping tools, data subject rights management tools, tools to support the development and implementation of the DPMP); and
- Access to external legal and technical advice.

Smaller organizations naturally have fewer resources for their DPOs. The ANPD should facilitate the ability of smaller organizations that need or desire a DPO to establish and train effective DPOs. This can be done for instance by providing clear and simple guidance focused on SME compliance; developing templates, tools and sample processes concerning DPO tasks; or offering relevant DPO training. In recognition of this, ANPD has included in its preliminary draft of the regulation for small data processing agents, subject to public consultation, an exemption for those agents from the duty to nominate a DPO.[16]

Further, depending on the ANPD's future resources, the ANPD might consider at an appropriate time whether to establish a specific ANPD department for DPOs with a single point of contact and dedicated resources. This would enable DPOs to have direct and easy access to the ANPD and would foster effective communication between the ANPD and DPOs. This would be particularly helpful for SMEs, but it should be open to organizations of all sizes. The French CNIL has established such a department. It is called the "Data Protection Officers Department". It consists of a team of legal experts that supports DPOs and leads actions for developing networks of DPOs based on sectors of activity (public bodies, business sectors, etc.) in coordination with the other departments of the CNIL.

3.8. DPO team and support from other corporate functions

Depending on their size and the complexity of their processing operations, organizations should consider applicable best practices relating to appointing a multi-disciplinary team to execute the DPO function under the leadership of the DPO. This team should collectively possess the range of skills necessary to exercise the DPO tasks. It could be composed of employees who have been moved from other functions of the organization to the DPO team, or it could be newly hired individuals or individuals taking the role on the DPO team in addition to their current responsibilities. For multinational organizations, the DPO team could be composed of individuals who are in different jurisdictions, as long as they are able to effectively exercise their designated DPO team roles.

Organizations can structure the reporting lines within these teams as most appropriate to their corporate structure. A hard reporting line to the DPO might be the most effective way to manage these roles in the DPO team. However, a dotted reporting line to the DPO for some of these team members such as those sitting in policy, product or legal functions could also work.

In addition to the core DPO team, larger organizations may also find it useful to appoint specific individuals within other corporate functions that are tasked with supporting the DPO team where required. They could have dotted reporting lines to the DPO for the part of their role that relate to

[16] ANPD, Minuta de Resolução [concerning the ANPD's regulations of SMEs], August 2021, available at https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/minuta_de_resolucao___aplicacao_da_lgpd_para_agentes_de_tratamento_de_pequeno_porte.pdf.

DPO support. For example, these could be lawyers within the legal function responsible for providing legal advice on privacy matters, or engineers within product functions responsible for explaining the technical aspects of products to the DPO team. Large organizations normally name such individuals as "Privacy Champions", "Privacy Officers" or "Privacy Leads" and provide them training on data privacy matters and opportunities to get certified.

Given that the LGPD provides for some specific obligations for DPOs, organizations should verify that any employee they appoint as DPO can also comply with the requirements of article 41 of the LGPD. Otherwise, organizations will have to provide other titles to these non-DPO employees who are tasked with privacy compliance to avoid misleading individuals, business partners and the ANPD that they are interacting with an official LGPD DPO.

Recommendations for the ANPD for its complementary rules concerning the role of the DPO:

- Consider establishing a specific department within the ANPD dedicated to engaging with DPOs.

4. THE TASKS OF THE DPO

The **main tasks for the DPO under the LGPD** are as follows:

- **Acting as the main point of contact between the organization and individuals** (Article 5, VIII and Article 41, paragraph 2)—this includes receiving and responding to queries and complaints from individuals concerning the organizations' data processing activities; being involved in the organizations' processes for handling data subject rights requests;
- **Acting as the main point of contact between the organization and the ANPD** (Article 5, VIII and Article 41, paragraph 2)—this includes being involved in any possible investigations or enforcement matters as well as on notifications to the ANPD of security incidents; being involved/consulted in any other formal and informal discussions between the organization and the ANPD (such as when the organization is show-casing their data privacy management program or informing the ANPD about any new/changed products and services); maintaining a trusted relationship with the ANPD; being easily accessible and available to the ANPD, as and when required; and
- **Providing advice and guidance to the organization on data protection and LGPD compliance** (Article 41, paragraph 2).

The fact that one of the DPO's core tasks is to act as the main contact point with the ANPD should not be viewed by organizations as an obstacle to the DPO being a trusted strategic business advisor to its organization. Also, this should not prevent other relevant functions and roles from being involved in the interaction, response, or meetings with the ANPD, or collaborating with the DPO in the organization's interactions with the ANPD. Where other functions engage with the ANPD, they should inform the DPO and/or coordinate with him/her/them in the engagement activities as appropriate.

Case study 5. Triaging individual complaints directed at the DPO

A multinational organization has a team dedicated to receiving and responding to complaints, queries and requests from individuals, including in relation to the exercise of their rights. This team has a process to triage and respond to such communications, and directing them to other relevant teams within the organization if necessary—including the DPO team, which is involved in higher-risk cases.

Organizations may also determine additional tasks for the role of the DPO (Article 41, paragraph 2). Of course,

additional tasks will depend on the needs of the organization, how the organization decides to establish the role of the DPO (more operational or more strategic), as well as the level of complexity and risks of their processing activities.

Some examples of **possible additional DPO tasks (or tasks in which the DPO could be involved) that have a more operational nature** are:

- **Maintaining records of processing activities** (Article 37);
- **Undertaking or supervising data privacy risk assessments** (Article 38);
- **Identifying the applicable legal bases for processing** (Articles 7, 11 and related Articles);
- **Drafting privacy notices to individuals** (Article 9);
- **Participating in the organization's response to and management of security incidents** involving personal data (Article 46)—including organizing table-top exercises with relevant internal stakeholders;
- **Undertaking or participating in audits of third-party** vendors' data privacy and security policies and procedures;
- **Drafting relevant internal policies, processes, controls and templates** for various data privacy matters and in connection with the organization's data privacy management program;
- **Drafting/negotiating Data Protection Agreements** ("DPA") with clients, partners and service providers; and
- **Providing training and planning awareness activities** for the various functions within the organization on data privacy matters.

Examples of **possible additional DPO tasks that have a more strategic nature** are:

- **Acting as a facilitator of, or being responsible for, the DPMP**—this can include a range of activities from program planning and development to program implementation and oversight; it could also include responsibility for implementing specific program work streams, (e.g., work relating to DPO responsibilities such as handling data subject rights requests and management of security incidents);
- **Overseeing the implementation of internal policies and processes relating to data privacy**—including undertaking periodic assessments and reviews; developing self-assessment tools to be used by the business; reporting on the effectiveness and completion of such policies and processes to senior management; advising on necessary updates to such policies and processes; supporting internal audits;
- **Being involved in key data privacy risk assessments** at various levels within the organization, including enterprise-wide as well as at the level of product/services and third party risk management—this includes being one of the key escalation points for product decisions needed following risk assessments; being involved in senior discussions concerning enterprise-wide risks;
- **Tracking national as well as global data privacy developments**—including analyzing the impact of such developments on the organization and reporting back to senior management; and

- **Being responsible for external engagement on data protection matters**—this includes attending and speaking at conferences, webinars or roundtables; reacting to media reports; providing feedback to senior management and relevant internal stakeholders on external stakeholders' sentiments towards the organization's data privacy practices; engaging in DPO networks/communities.

Recommendations for the ANPD for its complementary rules concerning the role of the DPO:

- Acknowledge that the DPO need not be involved in all data protection matters and leave it to organizations to define appropriate criteria for DPO involvement.
- Encourage organizations to adopt a risk-based approach towards the role of the DPO so that he/she/they are involved primarily in higher-risk and strategic matters.
- Provide flexibility for organizations to define their DPO's role in interacting with the public and the ANPD as appropriate to their business.
- Do not mandate additional tasks for the DPO that go beyond the core DPO tasks established by the LGPD—recommend and provide examples of additional tasks instead.

5. UNCERTAINTIES CONCERNING THE ROLE OF THE DPO UNDER THE LGPD

The role of the DPO has been long-established in some data protection laws. However, the DPO role is new in Brazil and Brazilian organizations have a series of questions about this role. In particular, because the LGPD's DPO provisions are flexible, they have left some issues open to the ANPD's further guidance (Article 41, paragraph 3 of the LGPD).

Naturally, organizations will be looking at international guidance and case studies in the absence of guidance from the ANPD. It is important, however, that they understand that there are substantial differences between the LGPD and the rules of other data protection laws, such as the GDPR, and that foreign regulations and case law will not be directly applicable to organizations in Brazil (except with respect to their cross-border processing activities). This section addresses some of the uncertainties that result from the absence of ANPD guidance and from the confusion concerning the applicability and relevance of foreign law, guidance and case law that might help organizations plan the role of the DPO.

5.1. Which organizations may be exempt from appointing a DPO?

Article 41, paragraph 3 of the LGPD establishes that the ANPD may issue complementary rules concerning the role of the DPO, including any exemptions from having to appoint a DPO. It is therefore not yet possible to fully address the question of which organizations may be exempt as it depends on the upcoming ANPD rules. However, we can provide recommendations for the ANPD to consider when drafting such rules.

Importantly, organizations that may be exempt under future ANPD guidance might still choose to appoint a DPO (or a person responsible for data privacy within their organization), as they might recognize that such a person will be of value in helping them meet their LGPD compliance and accountability obligations. Being exempt from the requirement of appointing a DPO does not mean that the organization will also be exempt from any other obligations under the LGPD, such as providing communication channels to enable individuals to exercise their data protection rights.

The ANPD should exempt organizations from designating DPOs based on the level of risk to individuals of their data processing activities. The risk may increase for example if the core of their business model consists of processing sensitive personal data. On the other hand, organizations that process low volumes of non-sensitive personal data (e.g., contact details) will likely have low-risk processing activities and could be exempted from having to designate a DPO. The ANPD should, as much as possible, facilitate such assessments, for example by providing a set of criteria, examples, case studies, checklists and templates.

Moreover, such guidance should prioritize or emphasize the needs of SMEs in determining whether they are required to have a DPO. In this regard, the ANPD has recently submitted to public consultation a resolution on small-sized processing agents—including micro and small business, startups, non-profit legal entities, natural persons and impersonalized entities that do not perform high-risk or large scale data processing activities— which provides that these processing agents are not required to appoint a DPO and may, alternatively, provide only a communication channel with the data subject.[17] A Public Consultation on the matter started on 30 August 2021 and CIPL responded to the preliminary phase of this public consultation.[18]

Also, the ANPD should encourage all organizations (regardless of whether they are exempted from the obligation to have a DPO) to train and upskill their employees in data protection matters, as well as to periodically re-assess the need to have a DPO to account for any changes in the risk level of their processing operations.

In addition, the ANPD should make clear that being exempt from appointing a DPO is an exception, rather than the rule. If the exemptions are too broadly cast to leave out a significant number of businesses that clearly would benefit from and could afford a DPO, then they run the risk of undermining the overall importance of the DPO, both with respect to the day-to-day compliance and operational functions and to the more strategic aspects of the role.

5.2. Are operators also required to designate a DPO under the LGPD?

The LGPD is not clear as to whether operators are required to appoint a DPO. While Article 41 specifies that controllers must appoint a DPO, Article 5, VIII defines the DPO as the person appointed by "the controller and the operator" to act as the main point of contact between the controller, individuals and the ANPD. The LGPD is also a risk-based legislation, meaning that to comply with a series of specific obligations, including designating a DPO (Article 41, paragraph 3), organizations should consider the level of risk to individuals of their data processing activities. In addition, the LGPD has a dual goal of protecting individuals' privacy and personal data while enabling technological and economic development (Article 2). Lastly, operators' clients will likely expect or prefer their vendor to have a DPO in place overseeing the operator's data processing activities.

The ANPD has issued Guidelines on Data Processing Agents and DPO which provides that, as a general rule, every organization shall indicate a person to assume the DPO role.[19] Therefore, we believe that operators should be encouraged to designate a DPO—and this DPO should act as the main contact point between the operator (as opposed to the controller) and individuals/the ANPD. Operators

[17] See footnote 16.
[18] CIPL Response to Brazil ANPD's Public Consultation on SMEs, March 2021, available in English https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[en]_cipl_response_anpd_public_consultation_smes_1_mar_2021.pdf; and available in Portuguese https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/[pt]_cipl_response_anpd_public_consultation_smes_1_mar_2021.pdf.
[19] See footnote 15.

appointing DPOs may facilitate the communication between operators and controllers, other operators, data subjects and the ANPD; facilitate cooperation with controllers to comply with the LGPD such as responding to data subject rights and managing data breaches; assist in contractual negotiations, among other benefits.

In any case, operators will likely always be controllers for some types of processing and types of personal data (e.g., HR processing of the operator's employees' data), and will have to designate DPOs for this purpose anyway if they are not exempted by future ANPD regulations. When a DPO is also required for the operators' non-controller activities, organizations should have the possibility to appoint the same person for both roles.

Further, it is possible to apply to operators the same rationale used to exemplify the case for SMEs above in that the ANPD may exempt SMEs from appointing a DPO if they undertake low-risk data processing activities. While some operators' data processing activities may represent a low-risk to individuals (e.g., an online system that provides table booking services to local restaurants processing only contact details of the restaurants' customers), other operators will have higher-risk data processing activities that will need more specialized, technical and strategic support from a data protection point of view. For example, several IT providers are large, multinational organizations that provide complex data processing services to their clients. Their data processing activities will likely fall under the medium/high-risk spectrum of a data protection risk assessment and they should be encouraged to designate a DPO under the LGPD.

Many operators understand that the designation of a DPO, as well as data protection accountability in general, is a competitive advantage and business enabler. Having a DPO would differentiate them in the marketplace and build trust in the digital supply chain with clients who are looking for accountable business partners to fulfil their own obligations. CIPL has found in a study that operators are taking steps to be accountable even when they may not be legally or contractually required to do so.[20] In fact, the LGPD also requires operators to implement data governance programs (Article 50), and DPOs have a key role to play in such programs, as seen in Section 2 of this Paper.

Finally, controllers and operators are also jointly liable for harms to individuals resulting from non-compliance with the LGPD (Article 42, paragraph 1), and having a DPO overseeing an operator's data protection activities may help reduce potential liabilities.

5.3. Should the DPO be an individual or could it be a department/team under the organization?

Traditionally, data protection laws around the world require that an individual should be designated to fulfil the role of the DPO. However, a question has arisen in Brazil as to whether a department under the organizations' governance structure, as opposed to a single individual, could be designated to fulfil this role. As the main interpreter of the LGPD, the ANPD could help answer this question in their upcoming guidance. When considering this question, the ANPD should acknowledge that the LGPD does not include a prohibition for the DPO to be a department/team under the organization. Some organizations may consider appointing a multi-disciplinary team to execute the DPO function under the leadership of the DPO, which should collectively possess the range of skills necessary to exercise the DPO tasks (see Section 3.8).

[20] See the CIPL White Paper What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework, May 27, 2020.

5.4. Can the DPO be a part-time role and/or an external DPO ("DPO as a service")?

Most organizations, especially large ones and organizations with higher-risk data processing activities, will establish the DPO as a full-time internal role as this will allow the DPO to develop the necessary knowledge of the business and its processing activities to perform his/her role effectively and also be fully accountable. The IAPP identified, in the aforementioned survey, that "sixty-three percent of the firms surveyed have their own in-house DPO, with another 8% outsourcing the role. Of those with an in-house DPO, most have just one, although about one-third of them have two or more."[21]

External and/or part-time DPOs can be particularly appropriate for SMEs, start-ups, NGOs (if they are required to appoint a DPO, considering the upcoming rules directed at small-sized processing agents) and other organizations that operate only in Brazil and that do not have complex processing activities or complex structures. Some start-ups may even choose to have a full-time DPO in their initial months of establishment of their businesses and move to a part-time DPO after the main data protection issues have been resolved. In any case, organizations should designate a DPO as appropriate to their specific context as long as the DPO can effectively exercise his/her/their tasks.

According to ANPD's Guidelines on Data Processing Agents and DPO, while the LGPD does not prevent the same DPO from acting on behalf of different organizations, it is important that he/she/they are able to perform her/his/their duties effectively.[22] Thus, before appointing a DPO, organizations should consider whether the DPO will be able to meet the organization's demands and those of other organizations at the same time. Also, the ANPD noted that the responsibility for personal data processing activities remains with the controller or the processor.

5.5. Should the DPO role have independence, protected status and avoid conflicts of interest?

In contrast to the EU GDPR, the LGPD does not explicitly require the DPO role to be independent or free of any conflict of interests. This question, however, often arises in Brazil as privacy practitioners and organizations look to the GDPR and its interpretation by courts and regulators to help them navigate the complexities of the LGPD. For example, one remarkable recent case involved a decision by the Belgian DPA that a company infringed the GDPR by appointing the Head of the Compliance, Risk Management and Audit department as DPO. The DPA understood that this position as Head implied that the individual makes decisions regarding the use of data within that department, which would be in conflict with the DPO role of providing independent oversight.[23]

This decision, however, should not impact Brazil, given that the LGPD does not require DPOs to be independent. In fact, the LGPD requirements for the DPO are quite different from the GDPR requirements in that they are simpler and more operational compared to the GDPR requirements, and organizations have more flexibility to specify other more strategic DPO tasks. In any event, organizations should consider it to be a good practice to ensure that their DPO is free of conflicts of interest to enable them to effectively exercise their statutory tasks. Organizations already apply this good practice in other functions, such as audit and finance. Therefore, organizations should consider possible conflict of interests when appointing a DPO and build relevant guardrails to ensure that the DPO is not placed in a position that could undermine his/her/their authority and legitimacy.

---

[21] IAPP-FTI Consulting Privacy Governance Report 2020, December 2020, available at https://iapp.org/resources/article/iapp-fti-consulting-privacy-governance-report-2020/.

[22] See footnote 15.

[23] See a summary at the Hunton Andrews Kurth's post on the Privacy & Information Security Law Blog on the Belgian DPA Sanctions Company for Non-Compliance with the GDPR's DPO Requirements, 6 May 2020.

5.6. Is the DPO personally liable for LGPD non-compliance?

The LGPD is silent on whether individuals, or professional firms acting as a DPO, can be subject to criminal, administrative and corporate liabilities. In other compliance areas (such as competition, anti-corruption and export control laws) of other jurisdictions such as the EU, compliance officers who take on roles that are broadly similar to DPOs are generally not subject to individual liability of any nature, except in cases of willful misconduct, gross negligence or breach of company policies or applicable law, just as any other employee would be.[24] This is also the case in Brazil, where the Civil Law ensures liability of employees that act with willful misconduct causing damage to the employer and third parties (Articles 186, 187 and 927 of the Civil Code—Law 10.406 of 10 January 2002).

Indeed, personal liability of the DPO would be inconsistent with his/her/their role under the LGPD as advisor to the controller or operator (Article 41, paragraph 2). This is because although DPOs provide advice, it is the organization that makes decisions concerning the data processing activities. Consistent with the controllers' and operators' obligation of accountability under the GDPR, controllers and operators carry responsibility for the data processing activities and, therefore, liability for non-compliance under the LGPD. In general, CIPL does not believe that there should be personal liability of a DPO under the LGPD as this may also dissuade many privacy practitioners from becoming a DPO and may dissuade companies opting to appoint a DPO when it is not required.

Again, in its Guidelines on Data Processing Agents and DPO, the ANPD noted that the responsibility for personal data processing activities remains with the controller or the processor.[25]

5.7. Should organizations publicly disclose the DPO's identity and contact details?

Article 41, paragraph 1 of the LGPD establishes that the identity and contact details of the DPO must be publicly disclosed, preferably on the controller's website. This issue is connected to the question of the DPO's personal liability as well as personal safety, and will require specific ANPD interpretation. We understand that when the legislature included this requirement in the law, its goal was to enable individuals to communicate with the organization concerning their data protection matters. There are many ways that organizations can enable such communications without publicly disclosing the personal details of the DPO (e.g., name, individual professional email address). Organizations can, for instance, create online forms dedicated to open a channel of communications between individuals and the organization, or publicize a DPO email address (as opposed to an individual email address). Publicizing the name of the DPO may lead to harassment of a DPO by a disgruntled individual or possible legal action against the DPO personally for the organization's failure to comply with the LGPD. This could discourage privacy practitioners from fulfilling the role of the DPO.

Case study 6. Organization decided to have DPO communications signed by the "Office of the DPO"

In order to prevent personal liability and relaliation to the DPO and protect the individual members of the DPO team, an organization has taken the decision that every communication that is sent from this team should be signed by the "Office of the DPO" instead of by the names of individual people working in this team.

[24] See the CIPL DPO Paper Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation, November 17, 2016.
[25] See footnote 15.

Additionally, the ANPD's Guidelines on Data Processing Agents and the DPO establishes that there is no need to communicate or register the identity and contact information of the DPO before ANPD, in view of the absence of legal or regulatory provision.[26]

Recommendations for the ANPD:

- Exempt organizations from the DPO requirement if their processing activities are low-risk.
- Encourage operators to appoint a DPO rather than making it mandatory in all cases.
- Allow a department within the organisation to fulfil the role of the DPO if appropriate.
- Allow organizations to appoint external DPOs if appropriate.
- Clarify that DPOs are not personally liable for the organizations' misconduct and non-compliance with the LGPD.
- Allow organizations to publish the contact details of the DPO office rather than the personal contact details of the individual fulfilling the role of the DPO to preserve his/her/their safety.

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

[26] See footnote 15.