



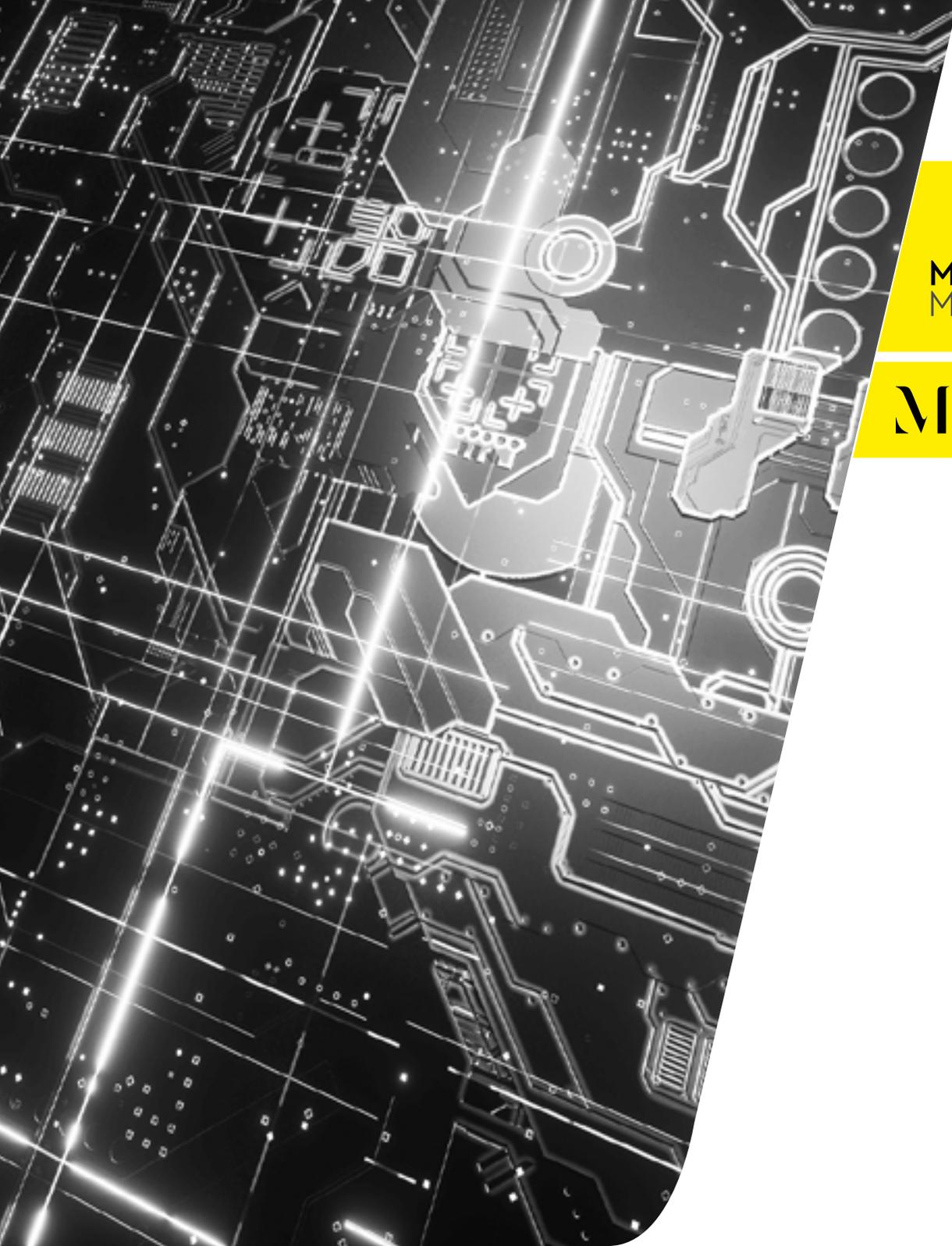
M



Machado
Meyer



M



PERSONAL DATA PROTECTION LAW: TRAVEL PLAN FOR MANAGERS

JANUARY DE 2019

CONTENT

	page
Introduction	3
1. In the internal plan	5
1.1 Transversal Application	6
1.2 Costs	7
1.3 Occam's Razor	8
1.4 Accountability	9
1.5 There are more questions than answers	10
1.6 Get to know your business	11
2. In the external plan	12
2.1 Celebrating a tie	13
2.2 Judiciary	14
2.3 Engagement	15
2.4 There are more questions than answers	16
Conclusion	17
Our contact information	18

INTRODUCTION

With the adequacy season to the Brazilian Personal Data Protection Law (Law No. 13,709/2018), aka LGPD, opened and reinforced by the creation of the National Data Protection Authority (or ANPD, Presidential Decree No. 869/2018), managers and organizations are being bombarded with risk analysis, recommendations, market solutions, and a multitude of information and cross-cutting discussions that, although relevant, may be of little use or even disrupt them, if they do not have the right mindset and travel plan.

It is a commonplace, but valid expression for our case: adaptation to the LGPD is a journey, not a destination¹. Thus, this article proposes a step prior to the discussions of a more technical legal nature for managers who need to face the LGPD as a practical, real, and immediate problem. What is suggested below is an initial travel plan on how to approach the LGPD from the point of view of organizations.

¹To paraphrase the English proverb "Life is a journey not a destination".

²Among others, see Müller, F. *Métodos de Trabalho do Direito Constitucional* ["Working Methods in Constitutional Law"]. 3rd ed., Rio de Janeiro: Renovar, 2005



What we have today, strictly speaking, is the legal text regarding the discipline of protection of personal data. There is, however, an important difference between the text and a legal norm. The norm corresponds to a systematic interpretation of the text of the law in its context, not to be confused, therefore, with the first². It emerges from the institutional and cultural background in which the protection of personal data in Brazil is found, as well as from the interpretation and application in question, especially by the ANPD and the Judiciary.

There is still a good deal of uncertainty about how the LGPD will actually be put into operation in Brazil; so prudence seems to be the order of the day. While awaiting the actual creation of the ANPD, recent news reports that the main party in support of the president of Brazil, with which he is affiliated, went to China in search of facial recognition technology to be used by the public authorities in cities to strengthen public safety³. There are serious questions about the (in)compatibility of the facial recognition model applied in China with the rule of law, which prioritizes the defense of fundamental rights and guarantees, including privacy and protection of personal data.

For all this, managers, when developing action plans to adapt an organization to the LGPD, need to keep their attention focused on both relevant environments of influence:

- the environment internal to the organization, which takes into account its strategy, structure, key processes, people, and skills.
- the external environment, which refers to the main stakeholders that interface with the organization, namely: ANPD, other government agencies, the Judiciary, clients, service providers, and competitors. Appropriate actions and an appropriate mindset will be necessary in both contexts. What I propose here, in a non-exhaustive manner, is to keep in mind certain considerations in relation to each of the plans, both the internal and the external ones, and to guide the actions for adaptation and technical aspects by these premises.

³ <https://noticias.uol.com.br/politica/ultimas-noticias/2019/01/16/bancada-do-psl-vai-a-china-para-importar-tecnicas-de-reconhecimento-facial.htm>



1

IN THE INTERNAL PLAN

1.1 TRANSVERSAL APPLICATION

The LGPD will be applied in a transversal manner. All businesses, albeit to a different degree, will be affected by personal data protection issues, even though from the point of view of technological development and innovation, issues such as IOT (Internet of Things), artificial intelligence, or machine learning are closely linked to the processing of data, including those of a personal nature.

The law has also adopted a principle of technological neutrality, such that, regardless of the methodology used in the processing, the rule will apply. In these terms, an organization's first job, especially the managers of

legal and information technology departments, is to show and convince the executive board that this is a strategic business issue, not a problem restricted to one or two departments, and which, therefore, should be seen as a multidisciplinary and structural project.

If there is no joint work by IT, engineering, legal, HR, product, business development, and marketing departments, etc., their adequacy project will invariably fail. A good start is to raise awareness among all teams and managers, as well as work on the formation of a multidisciplinary team, to, first of all, evaluate the business itself and its maturity with regard to the processing of personal data.

1 IN THE INTERNAL PLAN



1.2 COSTS

The adequacy process will not be painless. More than the financial cost of hiring service providers or procuring products to assist, there are significant organizational and cultural transformation costs that are less tangible but no less relevant.

Like any business problem, there are implications for strategic, structural, procedural, operational, and personnel issues. This scope will obviously be costly. The concepts of privacy by design and privacy by default brought in by the LGPD require that adequacy be considered of not only at the level of the product or service itself, but also from the organizational and procedural point of view. Structure, processes, practices, policies,

and a culture designed to favor the protection of personal data are demands brought about by the law, including in order to demonstrate compliance with rules and accountability.

The financial costs and less tangible costs that will be required in this process cannot be overlooked, and the timeline for this is short. This only underscores the fact that integrated and multidisciplinary work by an organization is the most efficient way to address adaptation to the LGPD. The more integrated the teams work, the more responsibilities are shared for the adequacy actions, the less costly the process as a whole, and it is inevitable that companies will consider these costs in their strategic, financial, and business objectives.



1.3 OCCAM'S RAZOR

This is not to say that the adaptation process will require extremely confounding and complex solutions. One should not expand the complexity and premises of a problem beyond what is necessary.

The best way to solve it is to seek a parsimonious solution, which includes only what is necessary. This logical and methodological principle should be applied in their adequacy planning.

Simpler solutions are important to reduce costs and are also the ones that best address the problems, especially when working in businesses of scale and with interdependent processes.

The indeterminacy surrounding the LGPD now demands a good deal of pragmatism. It is necessary to keep things simple and avoid a common approach in situations like these: creating difficulties to sell solutions. Start with the basics, form multidisciplinary teams, invest in knowing your own business model and how the personal data processing fits into it.

Understand what personal data is processed and map the cycle of this data within the processes and structure of your organization.

The LGPD contains in its article 6 a great compliance test. Make sure that your organization's personal data processing adheres

to the principles of the article and identify which ones for your situation are better or worse, prioritize based on that view, and work with a realistic timeline to address them. Article 6 of LGPD will invariably be an accurate thermometer of your level of compliance and risk. The adaptation period is not long and, in the face of open questions, it is unlikely to anticipate all necessary measures now. Follow the well-known prioritization matrix of looking first at the important, albeit at the expense of the urgent. Avoid getting lost in high complexities and theoretical discussions now. The LGPD is here to stay, but not all issues related to it will be resolved within the adaptation timeframe.

1.4 ACCOUNTABILITY

Liability and accountability are a guiding principle because they require that you not only comply with the other principles of the LGPD but also be able to demonstrate compliance with them.

A key question in adaptation concerns how the organization will be able to demonstrate compliance with the law. What policies, processes, documents, and other relevant evidence demonstrate adaptation.

It is important to remember that liability and the application of sanctions will be mitigated by the principle of accountability. Assuming that your organization will have some problem with personal data in the coming years (and we can be reasonably sure that this is a matter of when and not if), concern with this principle can make all the difference in imposing administrative sanctions and in future discussions of civil liability.

In addition, accountability is an important factor protecting the reputation of your organization and will help in matters not restricted to the legal sphere.



1.5 THERE ARE MORE QUESTIONS THAN ANSWERS

Brazil does not have a widespread culture of personal data protection. The level of concern of average Brazilians with what is done with their personal data is low.

The LGPD is a new text, inspired by a European directive (the GDPR) that results from a decades-long debugging process. Brazilian legislation is more general and open than the GDPR, and therefore has greater potential for indeterminacy and normative integration. We do not have settled case law on this subject and the ANPD has not even been formed.

Don't worry! This is not a call to despair, but to prudence. There are structural debates that we will have to go through. Even though it is a good text, the LGPD is not immune to problems, just like any legal text. Of course, there are choices and tradeoffs, but there are also inaccuracies, uncertainties, and potentially contradictions.

For example, is there room in the text to interpret the rules of civil liability in different ways (strict or fault-based liability? How will joint and several liability between processing agents take place?) That will have obvious consequences for businesses, depending on the interpretive path and integration adopted. Do not assume that experts know more about such a new subject in Brazil. There are no definitive answers for the moment.

1.6 GET TO KNOW YOUR BUSINESS

Before getting to know the LGPD it is important to have a diagnosis of the business. While everyone is somehow impacted by the law, the level of impact may be very different in each case.

So start by understanding the relationship between data processing and your business model: whether data processing is central in the strategic direction of your business, whether those skills need to be in-house or may be outsourced, whether or not the investment in a faster and more robust degree of adequacy can be a key competitive advantage.

For some, it is possible that adaptation is a cost to be absorbed (which needs to be done in the most efficient manner possible). For others, however, adequacy may be the strategic difference between success or disappearance.

There are organizations where processing of personal data is at the center of the business model, others may regard it as a very important but not fundamental item.

The determination of these situations is not only a legal or information security assessment, but rather a business diagnosis. And this can only be done in partnership with the different units of your organization.

Keep in mind that a law like this will have clear competitive impacts, it favors those who get ahead, and have more capital structure. Thinking about your competitive position is also critical.



2

IN THE EXTERNAL PLAN

2.1 CELEBRATING A TIE

There is some understandable celebration of the creation of the ANPD. Without it, the LGPD would be doomed to disorder or inapplicability.

But we must be aware that we are celebrating a tie. The ANPD does not have substantive independence, and the technical autonomy stated in the text is very doubtful without a budget.

We know that the effectiveness of the public administration is already challenging at the time the budget is provisioned. Without budgetary autonomy and without a more detailed design of its structure (the ANPD's regimental structure depends on an act of the President of Brazil), it is necessary to be very optimistic to believe that the body will be able to perform regulatory, auditing, and advisory functions to satisfaction. It remains to be determined who the board members will be and what profile they will have.

The ANPD has a lot of work to do, organizations' adaptation time is short, and a dialogue among players should have already been initiated in order to give proper progress to the process of adaptation to the law.

The agency is a stakeholder that deserves attention and with which organizations must engage, since the next chapters in its structuring will be fundamental in clarifying various points in the process of adaptation.

The good news is that Presidential Decree 869/2018 gave the ANPD the centrality needed to interpret issues relating to the protection of personal data. Parallel to its duty to coordinate with other government agencies, it was clear that the ANPD is the central agency for the interpretation of the LGPD, it has the assignment of regulation and implementation of the law (normative power) and is the agency that exclusively applies the administrative sanctions provided for by law.

2.2 JUDICIARY

In accordance with our constitutional system, it will be up to the Judiciary to resolve claims brought by owners of personal data. And as a result of the separation of powers, the Judiciary is not institutionally bound to any interpretation given by the ANPD. It will not be surprising if the Judiciary renders decisions diverging from the position of the ANPD in some cases⁴.

The issue of protection of personal data is new and complex, and it would be important to demand of the bodies responsible for the administration of the Judiciary an apparatus for preparation of judges who will soon come to adjudicate related cases. It is worth noting that the level of misunderstanding is not only that of trial judges.

A recent proposal by the National Council of Justice (CNJ) sent to the National Congress suggests as a method to help fight organized crime (purpose of the greatest urgency) the breaking of cryptography or backdoors, the maintenance in Brazil of a headquarters or representation for companies that provide messaging solutions, and the penalty of banning the services in the event of failure to comply.

No less troubling are previous precedents of blocking applications, such as those involving WhatsApp. Such proposals, in addition to being devoid of technical effectiveness (since criminals may rely on multiple messaging providers with end-to-end encryption), they weaken data protection and information security and end up damaging the vast majority of people who use these services for lawful purposes.

These are measures that bring about legal uncertainty and divert investments in Brazil as a consequence of the natural and justifiable mistrust of potential diverging positions on the part of local authorities. They are evidence that the Judiciary still has a good way to go in order to face issues of this nature.

In addition to demanding of the Judiciary better preparation on the subject, including in fields other than merely legal ones, engagement and much clarification work on the protection of personal data in the context of litigation will be necessary. This work needs to be thought out, planned, and structured right now.

⁴The declaration of invalidity of the US-EU Safe Harbor against Ireland's Data Protection Commission is a good example.

2.3 ENGAGEMENT

Discussions on personal data protection legislation go back at least to 2010, when the Ministry of Justice launched the first public consultation for the bill. In a process with many ups and downs, setbacks, and relevant facts⁵, low relative participation by the private enterprise marked the discussions.

For nearly nine years, much of the private sector remained stuck in the misguided view that personal data protection only affected the technology segment and therefore would not be a central concern. Others bet on the potential creation of exceptions for their respective industry. This lack of vision and participation was relevant in defining the paths that the legislative option took, including following the European data protection model to the detriment of other potential alternatives (which were never really discussed in Brazil).

⁵For more information, read Bruno Bioni's article on the topic: "De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados" ["From 2010 to 2018: the Brazilian discussion on a general data protection law"].

<https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018>

Only in the last year of the proceeding, at which time a good part of the proposals were already settled, was this absence partially mitigated. This is a mistake that cannot be made again. It is critical that organizations not only concern themselves with internal issues. Business sectors need to articulate their concerns, develop a concern for the ecosystem and influence governments, government agencies, and, in particular, the ANPD and the Judiciary, so that the implementation and regulation of the LGPD is rational and can in fact maximize the two objectives expressed in the text:

- the protection of fundamental rights and freedom, especially those related to privacy, self-determination, and freedom of expression.
- social and economic development, which depends on free initiative, free competition, foster innovation, and legal certainty and predictability.

2.4 THERE ARE MORE QUESTIONS THAN ANSWERS

The questions that are open to your organization are also put to your key stakeholders. In some cases, they may be similar, in others not, but your competitors, your service providers, your corporate clients, the Judiciary, the Executive, and the various government agencies that somehow relate to the subject are all in a learning phase.

Obviously, they face the subject of personal data protection according to their own perspectives, goals, and values. This phase is decisive because it will establish the framework and context of the law. From it we will move from the normative text to the legal norm and, in this sense, the result of what the LGPD will actually become is open and depends on the interaction of all these players.

Managers need to keep in mind that the process of creating the law is not over and that external engagement is as important as internal planning for adaptation.

CONCLUSION

Although not exhaustive, the comments made in this text may help managers to have a more organized framework to address different aspects of adaptation without forgetting what matters. After all, compliance with the law is not an end in itself, but a necessary exercise to ensure the achievement of your business goals, something your organization should not lose sight of in this process.



OUR CONTACT INFORMATION

DIEGO DE LIMA
GUALDA

PARTNER

dlgualda@machadomeyer.com.br
+55 11 3150-7774

LEGAL INTELLIGENCE PORTAL

Our view on issues that affect your businesses.

Access our content: www.machadomeyer.com/legalintelligence

MACHADO, MEYER, SENDACZ E OPICE ADVOGADOS
SÃO PAULO / RIO DE JANEIRO / BRASÍLIA / BELO HORIZONTE / NEW YORK

MACHADO
MEYER
.COM

