DIGITAL LABOR COMPLIANCE

SUMMARY

CONTACTS

GUILHERME DRAY
GDRAY@MACEDOVITORINO.COM

DENISE FINCATO
DENISE@DENISEFINCATO.COM.BR

1. INTRODUCTION

Labor Compliance does not limit itself to hard law, but also soft law, which does not arise from strict law and which, in an employment context, may address issues such as equality and non-discrimination, moral and sexual harassment, citizenship at work, etc. Generally, these recommended behaviors arise from codes of conduct, internal regulations and collective bargaining agreements.

Companies are obviously more skeptical when having to implement rules not imposed by law. However, this complementarity between what stems from hard law and what results from soft law is essential to comply with labor legislation, to close any gaps in the relationship between employee and employer, and to promote good working environments and employee well-being.

We have witnessed the increasing of awareness of companies' social, moral and environmental responsibility, within the concept of **ESG** (Environment, Social, and Governance), during the last decades, which has improved the enforcement of equality in the workplace as well as other issues related to citizenship rights, like harassment prevention and implementation of privacy policies and personal data protection.

With the implementation of compliance policies and with the companies 'concern to promote the "common good", reputational effects are now immediate which causes companies to become more appealing in the labor market, building a good working environment that will undoubtedly lead to the hiring and holding of talent and an increase in productivity.

In practical terms, labor compliance has meant the implementation of codes of conduct against harassment, on gender equality policies, including the tackle of pay gaps, the creation of whistleblowing channels to protect whistleblowers against retaliations in the workplace, as well as the creation of codes of conduct and ethics and compliance programs to prevent money laundering and corruption.

The obligation to adopt these soft law instruments, in some cases, arises from labor legislation or some separate pieces of legislation. In other cases, these policies stem from collective bargaining agreements negotiated between companies and unions.

2. DIGITAL LABOR COMPLIANCE IN BRAZIL

In Brazil, Law 12.846/13, known as the Anticorruption Law, regulated by Decree-Law 8.420/15, on the responsibility of legal entities for engaging in (harmful) acts against the public administration, highlights the importance of the adoption of an adequate Compliance program for Brazilian companies and the enforcement of an effective corporate governance system capable of implementing a culture of prevention and strengthening of transparency and ethics.

The Integrity Program, created by Decree-Law no. 8.420/15 in its chapter IV, article 41, by providing a set of procedures and integrity tools to be applied internally in companies to fight corruption, brought to the Brazilian legal system the first indications of the need to adopt a true Compliance program.

In this sense, Law no. 12.846/13 boosted the adoption of mechanisms inherent to Compliance by organizations, establishing the decrease of sanctions for companies that prove their cooperation in the investigation and analysis of violations, including the application of internal procedures of integrity and audit. The Law also encouraged the implementation of whistleblowing channels and codes of ethics, according to items VII and VIII, of article 7, tools common to the Compliance program.

3. MAIN NORMS AND INSTRUMENTS OF DIGITAL LABOR COMPLIANCE PROGRAMS, WHILE HIGHLITHING THE LGPD

To ensure the permanence of data and activities within the legal dictates, Compliance was accentuated in the digital environment with the entry into force of the General Law of Data Protection (**LGPD**), Law no. 13.709/2018, which came to show how important it was to adopt specific (and effective) mechanisms in integrity programs.

The scope of the incidence of **LGPD** entails the adaptation not only of the sectors related to the gathering of information, but also of the other operations that require the use of data related or relatable to natural persons, having repercussions, also and therefore, on labor relations.

In Brazil, privacy and intimacy are fundamental rights (art. 5, LXXIX, of CF/88), but unlike the **GDPR** (General Data Protection Regulation of the European Union), **LGPD** does not expressly mention its applicability to employment relationships, which is indisputable. Employment relationships could not even begin and develop without the processing of personal data collected at various stages of the employment contract of workers or job applicants. The legal gap pointed out allows the Brazilian legal system to be open to comparative law (art. 8 of **CLT**) and in contrast with the apparent lack of protection, international standards can be used in Brazilian labor relations.

Digital labor compliance plays a fundamental role, making it necessary to review conduct standards established for compliance with other norms, in order to avoid, for example, the collection of expendable data or data which processing may be considered discriminatory.

4. PRIVACY BY DESIGN E PRIVACY BY DEFAULT METHODS

GDPR introduced us to two new concepts, *Privacy by Design* and *Privacy by Default*. **LGPD** does not explicitly mention those concepts, but has adopted similar ones, when describing the measures that companies must implement to protect data, especially in article 46/2.

Privacy by Design means ensuring data protection from the beginning and can be better understood by looking at its seven informing principles. They are: (i) proactive rather than reactive, preventive rather than corrective; (ii) privacy by design; (iii) full functionality; (iv) end-to-end security; (v) visibility and transparency; (vi) respect for user privacy; and (vii) privacy by default.

One could say that Privacy by Default is an extension of Privacy by Design. The idea of Privacy by Default is that privacy should always be the default setting in any system or even business practice, and that the user should release access to collect more information if preferred, so that applications would collect only necessary information. In other words, the user's decision should always be respected (right to informational self-determination), since the data is the user's property.

The methods described above allow a beginning of a project already compliant to LGPD, reducing costs with later adaptation to the law.

5. POSSIBILITY OF INTRODUCING DIGITAL LABOR COMPLIANCE CLAUSES APPLICABLE TO EMPLOYMENT CONTRACTS

LGPD introduced the role of Data Protection Officer – (**DPO**) in Brazil, a person who acts as a communication channel between the institution, the data subjects and the National Data Protection Authority (**ANPD**). However, the legislator has preferred to be more flexible regarding the DPO when compared to other legislation, like, for example, the **GDPR**.

When it comes to data compliance in the workplace, there is no single implementation model to be followed, but there are three pillars that help: prevention, recognition and correction.

Prevention is considered the most important cornerstone, and it is up to the employer to invest most of their resources to ensure the security of their workers' information. The second cornerstone, recognition, is related to the existence of reporting channels as a form of control within the work environment. The correction cornerstone, on the other hand, establishes that any occurring breach must be immediately corrected.

The presumption of unevenness in employer-employee relationships is well known, making it unlikely for consent to be the sole and exclusive legal basis for workplace data processing, unless employees can withdraw it at any time and without adverse consequences, according to Opinion no. 2/2017 on data processing at the workplace, article 29 for data protection (employment group). Performance of a contract and legitimate interest can sometimes be invoked as reasons for data processing in employment relationships, provided that the processing is strictly necessary for a legitimate purpose and respects the proportionality and subsidiarity principles.

It should be noted that small businesses receive differentiated treatment, but are not exempt from complying with the provisions of the legislation at stake. The easing of the legislation for small businesses, in summary, refers to the simplification of data processing and the communication of security incidents (communication that can be made from the model made available by the National Data Protection Authority itself - according to Resolution CD/ANPD no. 2, January 27, 2022, which regulates the application of **LGPD** for small treatment agents).

6. PORTUGAL - DIGITAL COMPLIANCE AND DATA PROTECTION

"Compliance" is the mechanism used to achieve compliance (conformity) and to be compliant, so it can be both a means (to achieve compliance) and an end in itself (to be compliant).

Compliance can be legal, technological, administrative, among others, and is transversal to any organization, regardless of its public or private nature, area of activity and even size.

The compliance procedure, when directed to the cyberspace and digital environment, is nothing more or less than what we call digital compliance. In other words, the adoption of a set of rules, processes and procedures by companies to protect their data, which is one of their most valuable/ strategic assets.

For this reason, it is fundamental to integrate digital compliance into the business strategy of organizations. Any business activity necessarily implies processing operations of personal and non-personal data, which must be done in compliance with European and national legislation.

Regarding protection of non-personal data, the European Parliament adopted Regulation no. 2018/1807 of November 14, 2018, which was intended to promote the free movement of non-personal electronic data in the European Union. As opposed to "personal data," non-personal data is information that does not directly relate to an identified or identifiable natural person (individual). Examples of non-personal data are aggregated, and anonymous data sets used for big data analysis, in the current context of the strong expansion of the "internet of things", artificial intelligence, autonomous systems and 5G.

Regarding personal data protection, it is applied in Portugal the EU Regulation no. 2016/679 of April 27, 2016, which approved the GDPR and the Law no. 58/2019 of August 8, that ensures the enforcement of **GDPR** in Portugal.

Portuguese law, moreover, contains provisions on the protection of personal data specifically applicable to employment, including rules on the use of biometric data and on the means of remote surveillance, which are regulated.

To enable the implementation of these laws and regulations, international standards norms are created and modified, creating a correspondence between technical and legal norms.

ISO 27001 norm is one example.

The norm intends to enable public and private organizational environments to meet the data protection standards required by the **GDPR**, while seeking to summarize the union between the law, the information security and management and the information technology, which represents an evidence of digital Compliance.

In Portugal, with the pandemic scenario experienced recently, cyber-attacks have become more frequent, motivated by the exponential growth in Internet traffic and the adoption of telecommuting.

Given this, and in addition to the concern of complying with the legislation on data protection, digital compliance has been an increasing concern for companies, which seek to protect themselves, their employees, customers, suppliers and all those who interact with the company.

7. PORTUGUESE ANTI-CORRUPTION STRATEGY 2020-2024 (MENAC)

In Portugal, many measures have been taken to prevent and repress corruption and fraud in recent years.

However, the realization that only a long term vision, bringing together efforts and generating dynamics within the different powers of the State, the different areas of governance and the private and social sectors, would be able to confront the phenomenon of corruption, determined the need to design a National Anti-Corruption Strategy 2024 ("Strategy"), which enshrined as a priority the prevention and detection of "corruption risks in the public sector, through, among other measures, the adoption of Regulatory Compliance Programs in the Public Sector, based on the experience of the private sector" (Priority 2), as well as the need to "Engage the private sector in the prevention, detection and repression of corruption" (Priority 3).

Based on these priorities, some pieces of legislation were passed, namely, Decree-Law no. 109-E/2021, of December 9, which created the National Anti-Corruption Mechanism (**MENAC**) and the General Regime for the Prevention of Corruption (**RGPC**).

MENAC assumes the nature of an independent administrative entity, whose mission is to promote transparency and integrity in public action and to ensure the effectiveness of policies to prevent corruption and related offences.

MENAC holds powers of initiative, control and sanction, and is responsible, in particular, for: (i) developing, along with the Government, programs and initiatives for the creation of a culture of integrity and transparency, covering all areas of public management and all stages of education; (ii) developing campaigns for the prevention of corruption; (iii) collecting and organizing information on the prevention and repression of corruption and related crimes; (iv) issuing guidelines and directives for the design and terms of execution of regulatory compliance programs; (v) evaluating the application of **RGPC**; (vi) monitoring compliance with the norms set forth in **RGPC**.

In short: the creation of **MENAC**, stemming from the Strategy, intends to prevent and detect corruption risks in the public sector, and to engage the private sector in the prevention, detection, and repression of corruption.

8. THE FUTURE OF WORK AND THE RIGHT TO PRIVACY

With the increasing use of new technologies such as artificial intelligence, the so-called "Internet of Things" (**IoT**) and big data analysis, concerns about privacy, data protection and digital risks have increased significantly.

The digital revolution and its impacts on the labor market are likely to create risks to privacy and the protection of personal data, particularly in teleworking and remote working, as well as on digital platforms.

In fact, the new information and communication technologies place new means of surveillance of work activity at the employer's disposal, allowing more intrusive and permanent control, as well as almost unlimited processing of personal data.

This reality highlights the importance of protecting the right to privacy and the protection of personal data.

In Portugal, the Constitution of the Portuguese Republic provides for the right to privacy (Article 26) and the right to the protection of personal data (Article 35).

At the European level, the protection of privacy results from the European Convention on Human Rights (Article 7) and the Charter of Fundamental Rights of the European Union (Article 8).

The protection of personal data, in turn, results from the GDPR, which contains a specific rule regarding data processing in employment (article 88), as well as from Law no. 58/2019, which provides for specific situations of personal data processing, particularly in the context of employment relationships (article 28).

On a strictly labor level, it is also important to take into account articles 14 to 22 of the Labor Code, which include the right to privacy (article 16) and the protection of personal data (article 17).

Taking into account, in any case, the increased risks arising from the increment and massification of new technologies, the Green Paper on the Future of Work, approved by the

Portuguese Government in 2021, established new recommendations regarding privacy in the workplace, namely:

- Prevent and strictly regulate the practice of employment background checks, preventing the evaluation of the job applicant's profile and professional curriculum from being made using personal data of the applicant that have no direct connection with the type of activity for which he/she is applying and that interfere with his/her personal or intimate sphere;
- Prevent the use of tools that allow monitoring e-mails, websites visited, the amount of messages sent and calls/meetings held, originating a significant risk of remote surveillance of workers in real time, as well as enabling the creation of behavioral profiles.

The Future of Work is all about protecting the privacy and personal data of all parties involved, in particular workers.

9. CONCLUSION

In conclusion, to ensure the effectiveness of a Compliance program, it is essential to assess the risks involved and re-evaluate them continuously, since business is also in constant transformation, as well as technology, in order to prevent or mitigate damages resulting from the misuse or abuse of employee data.

In Brazil, regarding digital labor compliance, it appears that, although **LGPD** does not expressly establish provisions applicable to labor relations, the treatment of personal data is fundamental in the various stages of the employment contract, revealing itself, therefore, as a delicate area for its implementation and effective compliance. It can even be seen as an opportunity for the Brazilian legal system to open itself up to comparative law, namely, to the **GDPR**.

In Portugal, **GDPR** and national law that ensures its enforcement (Law 58/2019) have specific provisions for the employment context, which apply alongside the Labor Code, and whose compliance is indispensable to the implementation of a Compliance program.

Stakeholders have demanded parity of care in data handling, since liability for damages resulting from incidents is joint and several, and moreover, compliance with data subjects' data is a corporate value and strategic asset of organizations.

It is important that professionals in the labor area pay special attention to the obligations imposed by legislation and prepare to adapt their work routines/practices to data protection requirements, mainly through a risk management system to be integrated into an efficient digital Compliance program in the labor context.