Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Data Protection & Privacy 2022

Portugal: Trends & Developments

Pedro Lomba, Marta Salgado Areias
and Rita de Sousa Costa
PLMJ

practiceguides.chambers.com

Trends and Developments

Contributed by:
Pedro Lomba, Marta Salgado Areias and Rita de Sousa Costa
PLMJ see p.6

Portugal's Open Digital Economy

In today's global economy, data is an organisation's most critical asset, and companies face the significant challenge of handling data while ensuring data compliance. As a result, investment in infrastructure, such as European data centres, have increased greatly in recent years. This boom can be explained by the shift to cloud computing.

A tech-friendly country serving as a beacon for technological innovation both in the private and public sectors, Portugal is positioning itself to become a global player in hosting IT infrastructure and data management through cloud computing.

The country stood out in the 2020 edition of the European innovation scoreboard as it was the only "strong innovator" country to perform above the EU average in the "Innovation-Friendly Environment" parameter. Portugal has also signed up for the WIPO GREEN digital project (a marketplace for sustainable technology), which promotes the exchange of green-technology innovation between technological companies and partners that intend to sell, license or distribute green technology.

Furthermore, the Portuguese government has recently launched the Action Plan for Digital Transition, which is intended to support digital reforms in the economy and in the state.

This atmosphere of technological innovation is favoured by the significant openness of the Portuguese legal system.

Main Data Protection and Legal Privacy Framework

The main framework with regard to personal data in Portugal is the GDPR (General Data Protection Regulation) (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016), on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

As the GDPR gives room to the member states to implement specific provisions, Law 58/2019 of 8 August is the Portuguese law that ensures the execution of those provisions into Portuguese law. However, unlike the implementation law in other member states, the Portuguese law adds a few new provisions to the GDPR. The law ended up copying many of the provisions set out in the GDPR and this forced the authority responsible for supervising privacy and data protection legal frameworks (*Comissão Nacional de Proteção de Dados*, or CNPD) to state that it would not enforce these provisions by issuing Deliberation 2019/494. Law 59/2019 of 8 August implements Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Finally, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the E-Privacy Directive),

which is the lex specialis to the GDPR, was implemented in Portugal by Law 41/2004 of 18 August.

Direct Marketing

On 25 January 2022, the CNPD issued guidelines regarding direct marketing (Diretriz/2022/1), a matter that has been subject to a significant number of complaints. This is one of the few guidelines issued since 2018.

These guidelines advise organisations to revise their direct marketing practices. They also summarise the main topics of the applicable rules that result from the GDPR and Law 41/2004 of 18 August.

The document clarifies that when the controller and the recipient of the communications do not have a prior relationship, the only applicable legal ground is consent, despite Recital (47) of the GDPR. Under Article 13-A of Law 41/2004 of 18 August, controllers can only rely on a legitimate interest when they have obtained the contact details in the context of a previous commercial relationship, and if they send communications for direct marketing of their similar products or services. Furthermore, customers must clearly and distinctly have been given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when these are collected and on the occasion of each message if the customer has not initially refused such use. In other words, besides the requirements in Article 6(1)(f) GDPR and the required balancing test, these conditions also have to be met, and third parties other than the one that previously had the relationship with the customer cannot rely on a legitimate interest for direct marketing purposes. Instead, they can only rely on consent.

When consent is required, it must meet the requirements of Article 4(11) of the GDPR, and must be preceded by the necessary information to comply with Article 5(1)(a) and Articles 13 or 14.

The CNPD also stressed the responsibilities of controllers, even when marketing agencies or any third parties are responsible for marketing campaigns, and the need to comply with Article 28 of the GDPR and provide clear instructions. Third-party databases cannot be used unless consent has been obtained from one clearly identified specific entity.

To sum up – these guidelines refer to:

- the strict field of application of the legitimate interest ground for these purposes;
- the difficulties of using third-party databases;
- the fact that, even if third parties are responsible for the campaigns, the controller is still legally responsible; and
- the applicability of the additional requirements to the GDPR – provided by Article 13-A – to calls with human intervention.

Prior to the guidelines, this was not clear, because the provision only refers to automatic calls without human intervention, despite being merely exemplificative.

Data Protection Enforcement

Under the GDPR, national authorities have, inter alia, the power to:

- carry out investigations in the form of data protection audits;
- notify the controller or processor of alleged violations of the GDPR;
- obtain from the controller and processor access to all personal data necessary to perform their duties; and
- obtain access to all the premises of the controller and the processor, including the equipment and means of data processing.

The duty of co-operation imposed on public and private entities may lead to examination of data files and of documentation relating to the processing of personal data.

The supervisory authority also has the power to terminate or suspend the processing operations, should it consider that they infringe data protection law. Controllers and processors may apply to an administrative court for an injunction to overturn the administrative act issued by the authority.

In this regard, the CNPD has been taking a relatively soft approach when compared with other EU supervisory authorities (such as the Spanish AEPD, the French CNIL, or the Italian *Garante*) when enforcing the regulatory landscape. The CNPD has issued only a few guidelines since 2018. The supervisory authority has not yet published its plan of activities for 2022. However, the document for 2021 planned the issuance of guidelines regarding (i) the processing of children's data, (ii) cookies and (iii) privacy policies, and it is expected these could be issued during this year. The plan also included an assessment of the impact on the protection of personal data of the use, in new contexts, of artificial intelligence technologies, particularly machine learning, and the attention to be given, for the purposes of law enforcement and audits, to video surveillance in public areas, call centres, and the sharing economy's mobility platforms.

For example, according to data made available by the CNPD, there was a total of 34 fines in 2019 (up to EUR600,000). In 2020, the first year of the pandemic, there were 14 fines (up to EUR47,000).

However, while the official numbers for 2021 are yet to be released, it is fair to say that the activity of CNPD may be increasing. This can be seen in the very recent Municipality of Lisbon case. In this case, on 21 December 2021, the CNPD imposed a fine on the Municipality of Lisbon in the amount of EUR1.25 million for breach, inter alia, of the principles of lawfulness, transparency and the duty to provide information under Article 13 of the GDPR. This was a case in which the CNPD considered that there was a severe breach of personal data rules.

The most recent enforcement trends show that the CNPD tends to be more active in three situations:

- potential infringements committed by public entities, particularly against sensitive data;
- any case involving large volumes of data, that may appear en masse on a news outlet creating a situation of public alarm; and
- violations of Law 41/2004 of 18 August, regarding unsolicited communications.

International Data Transfers and Data Sovereignty in Portugal

An important feature of the Portuguese system is that, in contrast with other countries, Portugal does not have any specific law or provision establishing an obligation to process data in its territory.

Even with regard to special categories of personal data, such as health data, Portugal does not restrict the processing of such data to its territory, so the general rules on international data transfers apply.

This means that the main framework with regard to personal data is the rules laid down in Chapter V of the GDPR regarding international data transfers.

Following the Court of Justice of the European Union's (CJEU) C-311/18 Schrems II judgment, transfers to third countries or international organisations with the appropriate safeguards

under the GDPR have been subject to a threshold set by the CJEU. Portugal does not add anything new to the current EU legal practice and the CNPD has not issued any guidance in this regard.

However, the CNPD has been more active in the field of international data transfers, especially when sensitive data may be involved. Two emblematic cases in this respect are:

- the data protection order issued against *Instituto Nacional de Estatística* regarding the suspension of international transfers of personal data to the USA in the context of the Census 2021; and
- the "Respondus" case, an educational proctoring platform for universities, where the CNPD ordered the university concerned to stop using that platform.

While the authors of this article are aware that the Portuguese government has been working on a new national strategy for data, no substantial changes in this subject are expected. Nevertheless, according to Portugal's Cloud Strategy for the Public Administration approved in November 2020, data sovereignty may play a role when cloud service providers are offering services to the public administration. In other words, public administration bodies may be tempted to establish data sovereignty requirements when drafting tender specifications in public procurement procedures, which may affect the capacity of certain cloud service providers to compete by offering these services to those public bodies.

Finally, it is worth mentioning that no specific rules apply to non-personal data, notwithstanding the provisions of Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

All in all, this regulatory environment places Portugal as one of the countries with fewer regulatory constraints when it comes to data localisation requirements.

Data Protection and Cybersecurity

A final trend relates to cybersecurity. The beginning of 2022 was marked by several cyberattacks on media and telecommunications companies and the Portuguese Parliament's website. When it comes to the legal framework applicable in Portugal to cybersecurity, Law 46/2018 of 13 August implemented into national law the NIS (Network and Information Security) Directive (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016). In a similar vein, Law 65/21 of 30 July regulates specific aspects of Law 46/2018 of 13 August and defines cybersecurity certification obligations in implementation of Regulation (EU) 2019/881 of the European Parliament of 17 April 2019, thus providing for a high level of network and information system security within the country.

As the cybersecurity landscape is evolving, the European Commission has launched a proposal for a new NIS Directive (NIS2) intended to repeal the current one and enhance the level of cybersecurity in the EU.

Portugal benefits from the NIS framework and the European strategy to tackle cybersecurity threats and address both the cybersecurity and physical resilience of critical infrastructure and networks, which allows the EU to claim leadership in international cyberspace rules and standards. However, it is also true that organisations and companies are being confronted with the need to assess and improve the robustness of security systems in order to avoid security incidents and data breach incidents.

Contributed by: *Pedro Lomba, Marta Salgado Areias and Rita de Sousa Costa,* ***PLMJ***

PLMJ is a law firm based in Portugal that combines a full service offering with bespoke legal expertise. For more than 50 years, the firm has taken an innovative and creative approach to produce tailor-made solutions to effectively defend the interests of its clients. The firm supports its clients in all areas of the law, often with multidisciplinary teams, and always acting as a business partner in the most strategic decision-making processes. With the aim of being close to its clients, the firm created PLMJ Colab, its collaborative network of law firms spread across Portugal and other countries with which it has cultural and strategic ties. PLMJ Colab makes the best use of resources and provides a concerted response to the international challenges of its clients, wherever they are. Cross-border collaboration is ensured through firms specialising in the legal systems and local cultures of Angola, China/Macao, Guinea-Bissau, Mozambique, São Tome and Príncipe and Timor-Leste.

AUTHORS

Pedro Lomba is a partner and head of the Technology, Mobility and Communications practice at PLMJ. With over 17 years' professional experience as a lawyer, arbitrator and consultant, he specialises in information technology law, regulation, media and telecommunications law, internet law, mobility law, platform regulation, consumer law, advertising and data protection. His clients include both public and private bodies. Pedro is also a Professor at the Faculty of Law of the University of Lisbon. He has enjoyed a high profile in the media since 2004 and was a member of the Public Broadcaster's Public Opinion Council between 2016 and 2021.

Marta Salgado Areias is an associate in the Technology, Mobility and Communications practice at PLMJ who has five years' professional experience. She provides advice in the areas of privacy and data protection, intellectual property, consumer law and information technology. She has advised clients from various sectors of activity, including health, telecommunications, distribution and finance. Marta is a member of the International Association of Privacy Professionals and has completed a postgraduate course in intellectual law at the Faculty of Law of the University of Lisbon.

Rita de Sousa Costa is an associate at the Technology, Mobility and Communications practice at PLMJ. She provides regulatory, transactional and litigation advice in the areas of data protection, cybersecurity, media, advertising, consumer protection, smart mobility and emerging technologies. She has advised clients from the mobility, audio-visual and entertainment, life sciences, digital platforms for the sharing economy, software development and cloud computing sectors. She has authored and co-authored Portuguese and international peer-reviewed publications. Rita has also been panellist at international events and seminars in the intersection domains of law and technology.

PLMJ

Av. Fontes Pereira de Melo, 43
1050-119 Lisboa
Portugal

Tel: +351 213 197 300
Fax: +351 213 197 400
Email: plmjlaw@plmj.pt
Web: www.plmj.com

Transformative Legal Experts