An overview of GDPR compliance in Portugal

Tiago Félix da Costa
Partner, Morais Leitão
tfcosta@mlgts.pt

Maria da Assunção da Cunha Reis
Managing associate, Morais Leitão
macunhareis@mlgts.pt

How would you describe GDPR compliance supervision in Portugal?

From our experience, the Portuguese data supervisory authority (the *Comissão Nacional de Proteção de Dados* – CNPD) has been playing a reactive role, rather than an active one.

As a team also focused on regulatory litigation relating to non-compliance with the GDPR, we can conclude that so far CNPD acts mainly when confronted with complaints from data subjects, rather than proceeding with broad inspections on businesses and then applying measures deemed as necessary or initiating proceedings for violations of the GDPR as a result to those previous inspections.

The fact that CNPD acts on the data subject's complaints leads to us having most regulatory proceedings related to the non-compliance of the applicable rules on direct marketing, namely on relationships B2C.

In fact, most proceedings relate to the violation of rules provided for in the Law no. 41/2004, of 18 August (Telecommunications Privacy Act) and in a minor number with violations of the GDPR itself.

Can you describe the specificities of the rules applicable to marketing and direct marketing in Portugal?

In terms of the processing activities preceding the sending of direct marketing communications, the general rules of the GDPR apply, meaning that companies must determine the exact processing activities they perform for this purpose and then determine the applicable legal ground to proceed to such processing activities.

If no extensive profiling is made on the data subjects, companies normally tend to rely on legitimate interest to process the personal data for marketing purposes. In some cases, where there are extensive profiling activities, leading to the difficulty to defend that the legitimate interest of the controller overrides the data subject's rights and freedoms, or where such profiling can be included on the concept of automated individual decision-making (decisions taken with no human intervention which produces legal effects concerning the data subject or that similarly significantly affects him or her), companies sometimes rely on the data subject's consent to perform these processing activities.

As regards to the processing activity of sending the communications themselves, specific rules apply. According to article 13-A of the Telecommunications Privacy Act, you must collect the data subject's prior consent to send unsolicited communications (through automatic calling machines, email, or SMS) for direct marketing purposes. If the data controller has obtained the respective contact details from its customers in the context of the sale of a product or service, the data controller can then use them

> **Businesses more and more tend to rely on information – namely, information on their customers' wishes, needs and behaviours to develop products and services.**

for sending communications for direct marketing purposes, provided that (i) the marketing refers to its own products or services similar to those transacted, and (ii) it clearly and explicitly guarantees the customers in question the possibility of refusing, free of charge and easily, the use of such contact details at the time of collection, and at each communication, when the customer has not initially refused such use.

In a nutshell, to send direct marketing communications you can either rely (i) on consent (if you do not have a previous customer relationship with the data subject, or the products or services to promote are different from those previously acquired by the data subject), or (ii) on legitimate interest (if you have a previous customer relationship and the products or services you intend to promote are similar to those previously acquired by the data subject), depending on whether the requirements above are met.

As direct marketing has been one of the issues on CNPD's radar, CNPD has issued guidelines on this issue (Directive/2022/1 on electronic direct marketing communications). In these guidelines, CNPD mainly focuses on (i) the requirements to obtain valid consent from the data subjects for sending unsolicited marketing communications (which basically correspond to those set forth on the GDPR), (ii) the role of processors and the responsibilities of the controller when contracting those processors, and (iii) the specific case of acquiring data bases for marketing purposes.

What have been the main challenges for your clients on this topic?

Information is power. Businesses more and more tend to rely on information – namely, information on their customers' wishes, needs and behaviours to develop products and services. The more information you have, the most likely it is that you can create and sell a product or service aimed at people's wishes and needs and that can be of interest to the market. This understanding has led to marketing in more and more different ways being one key component of each business.

As such, the main challenge to our clients has been to ensure the compliance with the GDPR while taking action in processing data that is crucial to further develop their business. This means having to ensure transparency from the more operational areas, understanding the processing activities and then evaluate the risks and benefits from taking specific decisions towards such processing activities. The constant balance between the need to develop the business and taking risks in terms of data protection has been, from our perspective, the main challenge for our clients arising from the application of the GDPR.

We believe transparency is key. Providing clear and at the same time concise information to the data subjects can be a true challenge. The challenge is even bigger when the controllers have to explain profiling processing activities and/or algorithms' logic. In this light, EDPB and the data protection authorities should play an important role in setting and providing practical and usable guidelines to help businesses to achieve the desired levels of transparency.

The EDPB's recent guidelines on 'pay or ok' consent models have created significant legal and economic challenges in various markets. How is this reality seen in Portugal?

This type of model is still not widely seen in Portugal, but we admit that some digital services, and not just social media, will resort to this type of economic model.

> **Information on the data processing activities and ensuring a free consent are mandatory.**

In fact, if we think, for example, about traditional media, and the difficulties and challenges that digitalisation and the internet have brought to their sustainability and to the full application of their guarantees of independence and quality, it is very likely that this industry will have to resort to diversified models of remuneration, by creating and obtaining value, such as 'pay or ok' models.

From the point of view of national legislation, we believe that, in the abstract, there are no grounds for prohibiting this type of model, as long as the protection of personal data can be fully achieved, in accordance with the principles and rules of the GDPR.

In fact, the Portuguese followed the European legislator in the Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, as regards to the regulation of contracts where 'the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader', which are also regulated under the Decree-law no. 84/2021, of 18 October.

As the legislator has adopted the possibility of providing personal data in exchange for digital services, we can affirm that, in principle, the transfer of personal data or permission to process personal data as consideration for a digital service will be legally admissible and therefore 'pay or ok' models should be compliant.

Strictly speaking, as in other legal systems, citizens in Portugal are free to allow the economic and other uses of information that concerns them, as is the case, for example, with image rights. Having this in mind, we think that when it comes to 'pay or ok' models, the question will be how they can be used and not whether they can be used.

The consent granularity, information on the data processing activities and ensuring a free consent are mandatory. Controllers should find creative ways of achieving a compromise between the 'pay or ok' logic and privacy protection, notably by establishing more than one alternative to the payment of digital services and by ensuring that the 'pay' option is not too onerous for data subjects making it a real option.

Considering the importance of these models on the collection of data that can then be used for marketing purposes, we think that it will be a matter of time for these models to become being used by businesses. ■

M L MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS