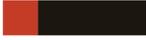


PORTUGAL



PLMJ 
SOCIEDADE DE ADVOGADOS, RL
A.M. PEREIRA, SÁRAGGA LEAL, OLIVEIRA MARTINS, JÚDICE
E ASSOCIADOS

Daniel Reis
Partner
T +351 213 197 313
E daniel.reis@plmj.pt



On the horizon

Protection of medical information

In 2014, the Portuguese Data Protection Authority (the CNPD) delivered a document to the Portuguese Parliament which highlighted the unconstitutionality of current legislation which allows entities, for example insurance companies, access to confidential medical information.

This access is possible due to the partial overlap of two laws, the Portuguese Data Protection Law (the DPL), and the Freedom of Information Act (the FIA) which regulates access to public sector information. Contrary to what happens in the DPL, the FIA establishes more flexible requirements for accessing public sector information, which can be consulted by anyone who has a “legitimate interest” in it. This has allowed insurance companies to access medical information about the National Health Service’s users without their consent, resulting not only in the violation of the DPL’s provisions on sensitive personal data, but also in the inequality of the level of protection of the patients’ medical information depending on whether they use public or private healthcare services. The aim is for the law to be changed during 2015 to ensure that all access to such sensitive personal data is subject to the DPL standards of protection and to the control of the CNPD.

Geolocation technology in the workplace

In November 2014, the CNPD published an opinion establishing the framework and conditions applicable to the processing of personal data collected through the use of geolocation technology in the workplace. These provisions focus on geolocation technologies used in devices made available by the employer to the employee, and particularly focussed on those used in motor vehicles and mobile devices, such as mobile phones, tablets and laptops.

Following this opinion, placing geolocation devices in motor vehicles is allowed for specific purposes only. In addition, the use of geolocation technology to monitor an employee’s professional performance or to monitor employees during their free time is strictly prohibited.

These provisions also introduce new information obligations: the employers are required to notify the employees of the use of geolocation devices and to inform them, in writing, of the conditions of and restrictions on use of any relevant equipment. Furthermore, the processing of employees’

geolocation data is subject to prior authorisation by the CNPD. The impact of these new rules will begin to be felt during 2015.

Cases

“Secretas” case

In 2014, the CNPD imposed a fine of EUR 4,5 million on Optimus, a Portuguese telecommunications operator, due to the infringement of data protection provisions. It was the largest penalty ever imposed by the CNPD.

The facts date back to 2010, when an Optimus employee delivered the communication records of a journalist’s mobile phone to an officer of the Defence Strategic Intelligence Service (part of the Portuguese Secret Services known as “Secretas”) who was trying to discover the journalist’s information source, because the journalist had released some classified information.

Optimus was found guilty of four offences: the lack of adequate measures to control data access by its employees; non-compliance with the data storage requirements; retention of data beyond the required time for retaining traffic data; and the failure to reconcile the rights of subscribers and the users’ privacy.

However, the telecommunications operator appealed to the Competition, Regulation and Supervision Court, which reduced the fine to EUR 600,000. Optimus then appealed again to the Court of Appeal of Lisbon, which issued the final decision in February 2015, setting the fine at EUR 100,000, as it considered that only one of the offences was proven (the fact that too many employees had access to the call records of customers, due to the lack of control measures).