Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cybersecurity

Second Edition

Portugal: Trends & Developments
SRS Advogados

chambers.com

2019

Trends and Developments

Contributed by SRS Advogados

SRS Advogados has a Data Protection and Cybersecurity team made up of five lawyers who have extensive national and international experience in the areas of privacy, data protection and cybersecurity. The team advises business groups and organisations on the implementation of the GDPR and related areas, and has also been involved in numerous M&A/private equity transactions in the cybersecurity space. The team adopts a multi-sectoral approach, focusing on finance and insurance, industrial, life sciences and healthcare, media and IT, and TMT/Digital. The Privacy and Data Protection practice works closely with other departments in the firm, namely in the areas of dispute resolution, administrative law and administrative offences. Key practice areas include handling data protection audits for the assessment of compliance with applicable rules (GDPR), advising on privacy and data protection policies, including the collection of data over the internet, and providing support on impact assessments and the management of security incidents/data breaches.

The team would also like to thank Sofia Riço Calado, Inês Maltez Fernandes, Mafalda Aguiar and Solange Fernandes for their contributions to this chapter.

Author

Luís Neto Galvão is a partner in the Corporate, Commercial and M&A Department, and is also the partner responsible for the Data Protection & Cybersecurity and TMT Departments. He has extensive experience in IT, telecommunications, media and privacy, and advises companies and organisations on privacy and data protection, including all aspects of compliance, data audits and international data transfers, especially in the telecommunications, media and IT, health and pharmaceutical, energy, banking and insurance sectors. Luís is also involved in the main projects in the area of Communications Regulatory, with a focus on the general authorisation regime and the grant of rights of use (spectrum and numbers), wholesale contractual relations among operators, regulated offers, interconnection and number portability, contracts with residential clients or companies, spectrum management and relations with the regulator ICP-ANACOM and the European Commission. He also worked intensively on the privatisation of a government-owned communications operator with listings in Lisbon, London and New York.

General Data Protection Regulation and Data Protection Law Enforcement Directive
The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) began to apply from 25 May 2018. Portugal has not yet enacted any national legislation to regulate certain aspects in connection with the GDPR, and a draft law prepared by the government is currently under discussion in the Portuguese parliament.

Among other issues, the new powers and status of the Data Protection Supervisory Authority (CNPD) need to be legally defined, in order to allow the CNPD to acquire the necessary human and financial resources to enforce the GDPR. The draft law submitted by the government faced significant criticism from the CNPD, including its intention to exempt public bodies from fines for a period of at least three years.

However, Portugal failed to implement in a timely fashion the Data Protection Law Enforcement Directive (Directive (EU) 2016/680) ('LED'). The European Commission has urged Portugal to implement the LED by the end of March 2019, failing which the matter will be referred to the Court of Justice of the European Union.

Supervisory Authority – CNPD
In spite of its current legal limitations, in October 2018, the CNPD applied a fine of EUR400,000 on the Hospital of Barreiro and Montijo ('CHBM'), under the GDPR.

Among other infringements, the CNPD considered that the CHBM had allowed indiscriminate access to its patients' personal data by third parties, such as social security officers, nutritionists, physiotherapists and psychologists, as well as by medical doctors who no longer worked at the institution.

The CHBM argued that the IT system it used did not provide the possibility to grant different levels of access to different professionals. However, the CNPD considered that such technical limitations could not jeopardise rights to data protection, namely, taking into account the fact that the CHBM never tried to resolve the issue with the Ministry of Health. In addition, it was found that the CHBM failed to erase user accounts of former practitioners in the hospital who had only provided temporary services.

The CNPD found that the CHBM had committed three infringements, namely:

- it failed to minimise data (Article 5(1)(c) of the GDPR);
- it did not apply adequate technical and organisational measures to ensure compliance with confidentiality and integrity principles (Article 5(1)(f) of the GDPR), and;
- it was unable to safeguard the confidentiality, integrity, availability and resilience of processing systems and services (Article 32(1)(b) and (d) of the GDPR).

The CHBM was regarded as acting with intent by enabling access to health-related data of thousands of patients. Furthermore, the CNPD had already warned the CHBM, in past decisions, about the need to employ a reliable audit system.

As mitigating factors, the CNPD highlighted the overall cooperating conduct of the offender, which tried to overcome its shortcomings even during the investigation phase, and the role to be performed by the Ministry of Health, which also had to intervene in monitoring access logs to IT systems. The first two infringements were subject to a fine of EUR150,000 each, and the third to a fine of EUR100,000, totalling EUR400,000.

The CNPD has also been challenged with a significant number of clarification requests concerning aspects of the GDPR. In addition, by mid-February 2019 it had received around 220 notifications of data breaches, according to the latest figures disclosed.

Practical aspects of GDPR
Following the GDPR's rule that allows each supervisory authority to set out the processing activities that should be subject to data protection impact assessments (DPIA), the CNPD approved Regulation No 1/2018, on the List of Processing Activities subject to Data Protection Impact Assessments. The transfer of health-related data through electronic networks, the linkage of special categories of data (eg, genetic data or biometric data) and the tracking of location and behavioural data for profiling purposes are some examples of processing activities that the CNPD has decided to subject to a mandatory DPIA.

The CNPD has also released, via its website, a notification form concerning the appointment of data protection officers and the disclosure of data breaches. The use of such forms is mandatory.

Finally, the CNPD has published model records of processing activities for both controllers and processors.

DECO against Facebook
The most significant Portuguese consumer protection association ('DECO') has brought an action against Facebook for illegal use of data from its users. Basically, according to DECO, personal data was collected for purposes not listed in Facebook's privacy statement, in contravention of the GDPR.

DECO argues that each user is entitled to compensation, which may vary depending upon the date of sign-in of the individual and the amount received for the data. On average, a given user may receive compensation of EUR200 per year of enrolment in Facebook. To date, more than 38,000 consumers have signed up to DECO's website in response to its announcement of the above-referred proceedings.

Cybersecurity and cyber-crime

The Portuguese Legal Regime of Cyberspace Security (Law No 46/2018, of 13 August 2018), has been adopted, transposing the Network and Information Systems Directive (Directive (EU) 2016/1148) ('NIS Directive'). This legal regime is applicable to public administration bodies, as well as to energy, transport, banking and financial market operators, the health sector, drinking-water supply and distribution-providers, digital infrastructures (eg domain name registries), online marketplaces, online search engines and cloud computing services.

All the above must take adequate and proportionate technical and organisational measures to manage the risks posed to network and information systems. Significant incidents must be notified to the Computer Security Incident Response Team (CSIRT) operating within the Portuguese National Centre for Cybersecurity (CNCS).

Failure to comply with the obligations of Law No 46/2018, of 13 August 2018, is an administrative offence, subject to a penalty of up to EUR50,000.

The 2017 Annual Report on Internal Security, published in March 2018, listed 1,895 notifications to CSIRT, of which 535 (28%) resulted in the opening of investigations. This figure represented an overall 50% decrease in notifications, when compared with 2016, and was due to a refinement of the screening process over the year.

This annual report also reported a widespread increase in cyber-crime, namely illegal access (21%), intrusion (16%), false representation (16%) and computer sabotage (27%). It foresees, as possible future trends, the rise of banking malware, money-laundering using bitcoins, general ransomware and sextortion.

SRS Advogados

Rua Dom Francisco Manuel de Melo, 21
1070-085 Lisboa

Tel: +351 21 313 2000
Fax: +351 21 313 2001
Email: geral.portugal@srslegal.pt
Web: www.srslegal.pt