Portugal's new data protection law in force since 9 August

Inês Antas de Barros and **Isabel Ornelas** of Vieira de Almeida explain the changes in the country's data protection framework. By **Laura Linkomies.**

The Data Protection Act was adopted in June 2019 signed into law by the President on 26 July 2019 and entered into force on 9 August 2019. *PL&B* put some questions to data protection experts, Inês Antas de Barros and Isabel Ornelas of Vieira de Almeida in Lisbon.

PL&B: Was the previous data protection law amended to comply with the EU Data Protection Regulation (GDPR), or is this a completely new text?

A new data protection law was published. Law 58/2019 (Portuguese GDPR Execution Law) revokes Law 67/98 of October 26 (the Personal Data Protection Act) and republishes Law 43/2004 of August 18, which regulates the organisation and operation of the Portuguese Data Protection Authority ("CNPD").

PL&B: How has Portugal applied the GDPR's derogations?

Although the Portuguese GDPR Execution Law addresses some of the GDPR's derogations (e.g. consent of minors and the imposition of fines in the public sector), there has been some criticism over the text of the law and the extent and material impact of its provisions.

Even Portugal Data Protection Authority, the CNPD has issued a formal opinion on the draft law, where it criticised the wording of the law, considering it to be a "word by word repetition of the GDPR" in some aspects, or a violation of the principle of EU law primacy (in the sense that it considers that some provisions contradict the GDPR).

PL&B: Would you say that, on the whole, the law follows the GDPR closely?

On the whole, the Portuguese GDPR Execution Law follows the GDPR. However, some provisions seem to exceed the wording of GDPR.

Indeed, various provisions have been recently considered by the CNPD to contravene the GDPR. The CNPD has issued Resolution 2019/494, determining that it will not apply certain provisions of the Portuguese GDPR Execution Law in the personal data processing operations it may assess. Such provisions cover: (i) scope of application, (ii) duty of secrecy; (iii) data processing by public entities; (iv) labour relations; (v) administrative offences; (vi) expiry of consent.

PL&B: Are there any differences from the GDPR in terms of national specifics in the law?

Yes, there are various provisions in the Portuguese GDPR Execution Law that differ from GDPR. We highlight the following: (i) the scope of application is extended (the law applies to personal data processing outside the domestic territory, when processed in the context of the activity of an establishment located on domestic territory); (ii) only in the case of intentional misconduct, does the law consider non-compliance with the principles of data processing, as a very serious administrative offence; and (iii) provision, as a very serious administrative offence, for refusal to cooperate with the CNPD.

PL&B: Is there a need to amend other laws as a result of the GDPR and this law?

The Portuguese GDPR Execution Law foresees that, with the entry into force of the GDPR, the legal provisions establishing the need to obtain an authorisation from the CNPD (or the need to notify this authority) automatically terminate. However, this general provision does not sufficiently address all contingencies and impacts of the GDPR in the national legal ecosystem. An in-depth analysis of the impact of GDPR on national laws and regulations should, therefore, be carried out.

PL&B: Is there a conflict with any other law?

The application of the Portuguese GDPR Execution Law poses some challenges to the harmonised and uniform application of legal provisions.

For example, the use of employee data in CCTV footage under the Portuguese GDPR Execution Law is not completely aligned with labour legislation and some current case law on the matter. Another example would be the articulation between the Portuguese GDPR Execution Law provisions on protection of deceased data subject data and the Portuguese legal framework on access to health data.

We anticipate that further challenges may be ahead, considering the impact of the Portuguese GDPR Execution Law and the fact that its application is still in its early stages.

PL&B: Is DPO autonomy defined? Are there requirements for qualifications?

The Portuguese GDPR Execution Law establishes that DPOs must perform their functions with technical autonomy. It is also foreseen that the DPO is appointed considering the requirements set by article 37/5 of the GDPR and no professional certification is required.

As to the DPO's functions, the Portuguese GDPR Execution Law extends the tasks of the DPO in the GDPR, further providing that the DPO shall (a) ensure periodic and unscheduled audits; (b) make users aware of the importance of the timely detection of security incidents and of the need to immediately inform the security officer; and (c) ensure communications with data subjects in matters covered by the GDPR and national data protection legislation.

PL&B: DPIA – has the office issued a list of when DPIA is required? Anything different from other EU Member States?

Yes. CNPD issued Regulation 1/2018 regarding the data processing operations that are subject to a DPIA. The list of mandatory DPIAs are quite well aligned with the lists issued by the other Member States, since it has taken into consideration the recommendations of the European Data Protection Board. In this sense, and without prejudice to the processing operations which are subject to the requirement of a prior DPIA already expressly foreseen in article 35 paragraph 3 of the GDPR, CNPD identifies the following nine processing operations which shall be subject to a prior DPIA:

1. Processing of information resulting from the use of electronic devices which transmit personal data concerning health via communication networks;
2. Combination of personal data or the processing which relates to personal data foreseen in article 9, paragraph 1 (sensitive data) or article 10 (criminal convictions and offences) of the GDPR or data of a highly personal nature;
3. Processing of personal data foreseen in article 9, paragraph 1 or article 10 of the GDPR or data of a highly personal nature based on its indirect collection, when ensuring the right of information pursuant to article 14, paragraph 5 (b) of the GDPR is not possible or feasible;
4. Processing of personal data which entails or consists of the establishment of large-scale profiles;
5. Processing of personal data which allows the monitoring of the location or behaviours of data subjects (for example, employees, clients or bystanders), and has as a result its evaluation or classification, except when the processing is essential for the provision of services specifically required by these data subjects;
6. Processing of the data foreseen in article 9, paragraph 1 or article 10 of the GDPR or data of a highly personal nature for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, except processing foreseen and regulated by law which presents appropriate safeguards for the rights of the data subjects;
7. Processing of biometric data for the unique identification of its subjects, when they are vulnerable data subjects, except processing foreseen and regulated by law which was preceded by a DPIA;
8. Processing of genetic data of vulnerable persons, except processing foreseen and regulated by law which was preceded by a DPIA;
9. Processing of personal data foreseen in article 9 paragraph 1 or article 10 of the GDPR or data of a highly personal nature with use of new technologies or new uses of already existing technologies.

PL&B: Has Portugal taken any measures for employee data?

Yes. The Portuguese GDPR Execution Law contains the following rules:

Employees' consent is not a lawful condition for the processing of their personal data (i) if the processing results in a legal or economic advantage for the employee or (ii) if such processing is necessary for the performance of the contract.

Recorded images and other personal data of employees recorded through video systems or other technological means of remote surveillance may only be used in the context of criminal proceedings and for the purpose of establishing disciplinary liability (insofar as they are used in the context of criminal proceedings).

The processing of the biometric data of employees is also limited, and may only be legitimately processed for two purposes: attendance control and access control to the employer's premises.

PL&B: What is the requirement for consent by children for provision of online services?

Children's personal data may only be processed by consent as provided for in the GDPR and concerning the direct provision of information society services, when such children have reached the age of thirteen. If the child is under 13 years old, processing is only lawful upon consent by the child's legal representatives, preferably through secure authentication means.

PL&B: What guidance has the Commission published so far on the new law?

The CNPD has issued several guidelines in respect of GDPR compliance (including on online processing of data by academic institutions, political marketing and distribution of electricity in smart networks[1]) and has also issued various documents aimed at assisting companies with GDPR compliance – for example, data breach notification templates, DPO appointment notification and data processing registry templates.

The CNPD has not issued specific guidance on the interpretation and application of the new law, insofar as it has not provided public and formal information on how to apply the law and how companies should address specific provisions within the law. However, as noted above, the CNPD has issued a decision concerning its approach to several provisions in the Portuguese GDPR Execution Law, expressly determining that CNPD will not apply certain articles in this law – rather, where applicable, it will apply GDPR provisions, directly and without regard to the Portuguese GDPR Execution Law.

PL&B: Did the commission have fining powers before?

Yes, CNPD already had – and exercised – fining powers under the previous law, although the amounts were significantly smaller than those set out in the GDPR, since maximum penalties per event of breach were capped at 30.000 (except in the event of a breach in e-privacy, which was subject to a specific law and to heftier fines).

PL&B: Has the DPA issued any monetary penalties so far?

Yes. According to the information publicly available at CNPD's website, CNPD has, so far, issued four penalties concerning: (i) non-compliance with the obligation to implement appropriate organizational and security measures; (ii) non-compliance with the obligation to provide to data subjects the necessary information (CCTV); (iii) non-compliance with the obligation to comply with data subjects' rights.

PL&B: Do you know if the DPA is planning audits? In which sectors?

Yes, we understand that CNPD is planning various audits to monitor GDPR compliance.

CNPD has not provided specific indication of which entities/sectors would be the target of these audits, but CNPD has been focused on regulated sectors (such as health, insurance and finance) and on specific types of processing (particularly direct marketing and the processing of special categories of data), so monitoring actions may focus on these.

PL&B: Are previously obtained consents valid?

The Portuguese GDPR Execution Law establishes the same rule as the GDPR. Consents previously obtained are valid, provided that such consents comply with GDPR requirements.

PL&B: Please explain this new concept of data rights for the deceased. How does the right of access, rectification and Right to be Forgotten (RTBF) work in this context?

The Portuguese GDPR Execution Law includes a specific provision on the processing of data for deceased persons, stating that this data is protected under both the GDPR and the Execution Law, whenever this data either constitutes special categories of data under article 9 of the GDPR, or when they refer to the person's private life sphere, image or communication data – without prejudice to the derogations in paragraph 2 of article 9.

In this context, the Portuguese GDPR Execution Law foresees that data subject rights - namely the right to access, rectification and deletion - may be exercised by the person previously indicated by the deceased or, when no such appointment was made, by his/her heirs. However, data subjects also have the right to decide that, upon their death, data subject rights may not be exercised.

PL&B: What is specified on data retention periods?

The Portuguese GDPR Execution Law establishes some specific rules concerning data storage. In particular, it provides that, with respect to personal data processed for purposes of scientific or historical research as well as for statistical purposes – where it is impossible to previously determine the moment when such processing is no longer necessary - their storage is lawful, provided that adequate technical and organisational measures are adopted to guarantee the rights of the data subject, namely the information on their storage.

It further provides that where data proves necessary for the performance of contractual or other obligations, such data may be retained until the respective rights become time-barred.

INFORMATION

Inês Antas de Barros is Managing Associate and Isabel Ornelas is Senior Associate at law firm Vieira de Almeida, Lisbon, Portugal. www.vda.pt
Emails: iab@vda.pt
igo@vda.pt

REFERENCE

1 This is a reference to the CNPD's 2/2019 Guidelines on intelligent electric energy distribution networks, which, through smart meters, process personal data whenever the final consumer is an individual person – for example, energy consumption data, relevant usage period and consumer profiling.
The Guidelines were aimed at clarifying the legal grounds for the processing, terms in which data subjects could exercise their rights and minimization of impact on data subjects – particularly considering a need to balance regulatory obligations in the energy sector, technological features of the equipment and GDPR principles.

Companies found in violation of Privacy Shield

The US Federal Trade Commission (FTC) filed, on 24 July, an administrative complaint against data analytics company Cambridge Analytica which also states that Cambridge Analytica falsely claimed that it was a participant in the EU-US Privacy Shield. In fact, its certification had lapsed in May 2018. Earlier in July, the FTC reached a settlement with a background screening company SecurTest over allegations that it falsely claimed to be a participant in the EU-US and Swiss-US Privacy Shield Frameworks.

But the Electronic Privacy Information Center (EPIC) criticised the decision saying that while the settlement requires SecurTest to halt misrepresentations and submit to compliance monitoring, it provides no remedy to those EU citizens who used the service.

EPIC and other commentators have pointed at the absence of a comprehensive US federal privacy law and a data protection authority. The Third Annual Review by the EU Commission on the functioning of the EU-US Privacy Shield is due to take place in October.

- *See www.privacyshield.gov/NewsEvents and epic.org/2019/08/company-violates-privacy-shiel.html*

Gibraltar joins Convention 108

Council of Europe Convention 108 will enter into force with respect to the UK Territory of Gibraltar on 1 November 2019. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – known as Convention 108 – provides for free flow of personal data between states party to the Convention. Gibraltar has had a data protection law since 2004 (*PL&B UK Report* June 2006, pp.10-11).

- *See www.coe.int/en/web/data-protection/-/convention-108-welcome-to-gibraltar*

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Thailand – Asia's strong new data protection law

The law which will enter into force in May 2020 includes many GDPR-informed principles, but also some omissions.
By **Graham Greenleaf** and **Arthit Suriyawongkul**.

A military coup in 2014 imposed a junta government in Thailand. In February 2019, three weeks before the first general elections since the coup, this government enacted a data privacy law to override an old and ineffective law applying only to the public sector. A military-backed party now leads a coalition government with a Prime Minister and Cabinet members from the previous military

Continued on p.3

CNIL's guidance on cookies sets stricter consent requirements

Web publishers need to adapt their websites to France's new rules. **Ariane Mole** and **Juliette Terrioux** of Bird & Bird explain.

On 4 July 2019, France's Data Protection Authority (the "CNIL") adopted new guidelines on cookies and similar technologies[1], which replaced the previous guidance published by the CNIL in 2013[2].

The major change concerns the means to obtain a valid consent from users. The consent of users can no longer result from their browsing on the website. Web publishers will now have to comply with stricter requirements for users' consent.

Continued on p.7

Future PL&B Events

- *Asian data privacy laws*, 30 October, Linklaters, London
- *New Era for US privacy laws: California and more*, 14 November, Latham & Watkins, London.
- *Balancing privacy with biometric techniques used in a commercial context*, 29 January 2020, Macquarie Group, London.
- *PL&B's 33rd Annual International Conference*, St. John's College, Cambridge 29 June to 1 July 2020.

privacylaws.com

Issue 161 OCTOBER 2019

INTERNATIONAL report

ISSUE NO 161 OCTOBER 2019

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Ariane Mole and Juliette Terrioux
Bird & Bird, France
Guoda Šileikytė
WALLESS, Lithuania
Jay Fedorak
Office of Jersey's Information Commissioner
David Barnard-Wills
Trilateral Research, UK
Arthit Suriyawongkul
Foundation for Internet and Civic Culture, Thailand
Inês Antas de Barros and Isabel Ornelas
Vieira de Almeida, Portugal
Wenlong Li
University of Edinburgh, UK
Alvin Cheung
University of Oxford, UK

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

From Thailand to Jersey – GDPR's global effect is evident

Our Asia-Pacific Editor, Graham Greenleaf writes in this issue that the Thai data protection law is the first explicitly "GDPR-based" law yet be enacted in Asia (p.1), and Jersey's Information Commissioner, Jay Fedorak says that Jersey's close alignment with the GDPR forms part of a general economic strategy (p.12). It is therefore clear that the GDPR is having a global effect – also in Australia where there are pressures to modernise the law (p.17).

In our series of GDPR implementation across EU Member States, we now turn to Portugal. Its law, adopted in June this year has been in force since August. Read an interview about the law with Portuguese DP lawyers on p.14. In Lithuania, a new data protection law was adopted in June 2018, and the regulator has now issued the first significant fine. There are some national specifics that are different from the GDPR such as the provisions regarding the processing of national identity numbers (p.9).

Meanwhile, organisations need to get on with training. The STAR project's ready-made, easy-to-customise training materials, developed for the busy DPO, are now available (p.20). The STAR training materials are based upon research into existing GDPR training practices and should therefore be relevant and very useful.

We also return to the issue of recent cookie guidance from France's regulator (p.1). Things are moving fast in this area – the Internet Advertising Bureau Europe has released the second version of its consent and transparency framework, and Google has said it expects to join by the end of next March.[1]

We are also pleased to bring you the winning competition essays from PL&B's Student Essay Competition this summer. These two winning entries discuss consent, legitimate interest and joint controllership in AdTech (p.24), and the market and legal challenges in convincing companies that GDPR-compliance is a competitive advantage (p.28).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

1 digiday.com/media/google-to-join-iabs-revamped-gdpr-framework-by-next-march/

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 165+ countries alongside legal analysis, management guidance and corporate case studies.

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 165+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and administrative decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

6. Back Issues
Access all *PL&B International Report* back issues.

7. Events Documentation
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"*PL&B's International Report* is obligatory reading for our team members worldwide to keep them up to date on relevant developments in other jurisdictions. Concise but always precise!"

Professor Dr. Patrick Van Eecke, DLA Piper

UK Report

Privacy Laws & Business also publishes *PL&B UK Report*, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.