THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

FOURTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE Privacy, Data Protection and Cybersecurity Law Review

Fourth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2017
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LawReviews

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

ACCOUNT MANAGERS
Pere Aspinall, Sophie Emberson,
Laura Lynas, Jack Bagnall

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Arthur Hunter

EDITORIAL COORDINATOR
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Robbie Kelly

SUBEDITOR
Caroline Fewkes

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-910813-89-8

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© 2017 Law Business Research Ltd

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC–PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

THE ISLAMIC FINANCE AND MARKETS LAW REVIEW

THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW

THE CONSUMER FINANCE LAW REVIEW

THE INITIAL PUBLIC OFFERINGS REVIEW

THE CLASS ACTIONS LAW REVIEW

THE TRANSFER PRICING LAW REVIEW

THE BANKING LITIGATION LAW REVIEW

THE HEALTHCARE LAW REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BAKER & MCKENZIE – CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

DUCLOS, THORNE, MOLLET-VIÉVILLE & ASSOCIÉS (DTMV)

JUN HE LLP

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP J

LEE & KO

M&M BOMCHIL

NNOVATION LLP

PERCHSTONE & GRAEYS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VDA VIEIRA DE ALMEIDA

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 21

PORTUGAL

Magda Cocco and Inês Antas de Barros[1]

I OVERVIEW

Data protection and privacy are deemed to be fundamental rights recognised by the Constitution of the Portuguese Republic.

The protection of the privacy of home and correspondence privacy is set forth in Article 34[2] and Article 35[3] of the Constitution, which establish the foundations for the protection of personal data.

Following the EU approach, Portugal has an omnibus data protection legal framework that generally applies to both private and public sectors, as well as to any sector of activity: the Data Protection Act, approved by Law 67/98 of 26 October 1998 (the Data Protection Act).[4,5] This legal framework transposes into Portuguese law Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Further to the approval and entering into force of the General Data Protection Regulation (GDPR) on 25 May 2016, Portugal has now begun a process of adjustment to the profound changes that this new law will bring directly upon its application from 25 May 2018 onwards. Until then, the Data Protection Act will continue to apply.

As regards the electronic communications sector, Portugal has approved Law 46/2012 of 29 August (the ePrivacy Act) concerning the processing of personal data and the protection of privacy.[6]

---

1 Magda Cocco is a partner and Inês Antas de Barros is a managing associate at VdA Vieira de Almeida.

2 The Constitution recognises that an individual's home, and the privacy of his or her correspondence and other means of private communication, are inviolable. It prohibits anyone entering the home of any person without his or her consent except by order of the competent judicial authority, and in those cases, according to the forms laid down by law. It also prohibits any interference with correspondence or telecommunications, apart from in those cases laid down by law in connection with criminal procedures.

3 Article 35 provides that every citizen shall possess the right of access to all computerised data that concern him or her, to require that they be corrected and updated, and to be informed of the purpose for which they are intended, all as laid down by law.

4 The Data Protection Act replaces the 1991 Act on the Protection of Personal Data with regard to Automatic Processing, which was enacted to implement the requirements of the 1995 Data Protection Directive and later amended by Law 103/15 of 24 August.

5 As amended by Law 103/15 of 24 August.

6 It transposes the part of EU Directive 2009/136/EC amending EU Directive 2002/58/EC of 12 July concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The CNPD, the Portuguese data protection authority – the entity in charge of supervising the application of the regulations on data protection – was created in 1991. It is an independent body with powers within the scope of the Assembly of the Republic, the national parliament.

In recent years, and taking into account the legal and practical evolution of the data privacy framework, data privacy has increasingly become a priority and a concern to market participants in all areas and sectors of activity. However, there are still steps to be taken to ensure that all market participants are duly aware of the possible impact of a data privacy breach – legally, financially and in terms of commercial strategy.

Recent cyberattacks on many Portuguese private companies and public entities have caught the attention of the media, and these, along with the annual national cyberdefence and cybersecurity exercise organised by the Portuguese army, have contributed to creating awareness and know-how on cybersecurity and cyberdefence.

While there is no general cybersecurity or cyberdefence legal framework, there is sectoral legislation concerning the security of communication services and networks.

II THE YEAR IN REVIEW

In the past couple of years, the CNPD has issued several opinions that received wide media attention.

In 2015, the CNPD conducted an audit of the Portuguese Tax and Customs Authority (the Tax Authority) following the creation of a 'VIP list' (a list concerning a special group of taxpayers composed of public figures linked to politics and sports). The CNPD concluded that no adequate security measures had been adopted and, therefore, confidentiality was compromised. Also in 2015, the CNPD issued several opinions, including Opinion 1704/2015 on the processing of personal data within clinical investigations; Opinion 1450/2015 on access to data from the electoral registration database; and Opinion 1770/2015 on the intra-group agreements review procedure for transfers of data outside the EU. In 2016, the CNPD issued Opinion 923/2016 on the access of executive officers and solicitors to the personal data included in employees' payslips in the course of executive processes, and an Opinion[7] on a legislative proposal to provide the Tax Authority with access to bank account data. In July 2017, the CNPD approved Opinion 1039/2017 on the Principles Applicable to the Recording of Phone Calls, revising Opinion 629/2010. In this document, the CNPD defines new time limits for the retention of call recordings for the purpose of proving commercial transactions and any other communications regarding the contractual relationship.

In terms of enforcement actions, in recent years, there has been a clear trend on the part of the CNPD to be more proactive.

In relation to the implementation of the GDPR, the CNPD approved and published a document in January 2017 establishing 10 measures to be taken by entities to prepare for the application of the GDPR. The CNPD has highlighted the main areas of intervention and set out some actions to be taken to ensure compliance with the new legislation. The CNPD will continue issuing guidelines on the GDPR with the purpose of ensuring that it is applied uniformly by the organisations affected. Recently, in August 2017, the government approved Order 163/2017 creating a working group with the purpose of preparing the Portuguese legislation for the application of the GDPR in Portugal.

7 To date, this Opinion has not been published.

As to cybersecurity, in 2015, 2016 and 2017, several attacks on the information systems and websites of public entities were reported, leading to the defacement of websites and disclosure of confidential information. One such attack in 2016 was perpetrated against the information systems of the parliament, the Supreme Court and the police. Following their creation in 2014, the implementation process of the National Cybersecurity Centre and the Cyberdefence Centre continued in 2015 and 2016. In 2015, the National Cyberspace Security Strategy was enacted, setting out the main principles for network and information security, and proclaiming the strategic importance of cybersecurity and cyberdefence in Portugal.

In 2017, the National Cyberspace Security Strategy was approved with the purpose of further developing network and information security, ensuring the defence and protection of critical infrastructure and vital information systems, and enhancing a free, secure and efficient use of cyberspace by all citizens, and by companies and private and public entities.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

In Portugal, the legal data protection framework is regulated by:

a Article 35 of the Constitution;
b the Data Protection Act;
c the ePrivacy Act; and
d Law 32/2008 of 18 July, which sets out the data retention obligations imposed on providers of publicly available electronic communications services.[8]

There are also data protection provisions in other sector-specific regulations, such as, *inter alia*, the regulations concerning clinical trials, genetic information and anti-money laundering. The Data Protection Act, applicable until the date on which the GDPR will apply (25 May 2018), aims to protect an individual's right to private life while processing personal data, establishing the rights and associated procedures of natural persons (data subjects), and the rights, duties and liabilities of legal and natural persons when processing personal data.

'Personal data' is defined as information of any type, irrespective of its medium, including sound and image, relating to an identified or identifiable natural person (data subject). Two categories of data set out in the Data Protection Act are classified as sensitive data and require special treatment: (1) data relating to an individual's philosophical or political beliefs, political party or trade union membership, religion, racial or ethnic origin, health or sex life, including genetic data, and private life data; and (2) data relating to criminal and administrative offences, legal decisions applying penalties or suspected illegal activities.

The controller is the entity directly liable for compliance with the data protection rules. Omission or inadequate compliance with the rules set forth in the Data Protection Act may result in civil or criminal liability or a fine of up to €29,927.88 (up to €5 million under the ePrivacy Act).

Additional penalties may apply, such as data blocking or destruction, temporary or permanent prohibition of processing, or publication of the judgment.

8 The validity and enforceability of this Law (as well as corresponding laws in the EU territory) has been uncertain since April 2014 when the Court of Justice of the European Union (CJEU) invalidated Directive 2006/24/EC (which is transposed by this Law) for violating fundamental rights.

ii General obligations for data handlers

The Data Protection Act sets out principles and obligations that data handlers must comply with when carrying out personal data processing,[9] with controllers and processors having different statuses.

Obligations of data controllers

The controller has a large number of obligations. In particular, the controller shall ensure that:

a personal data are collected and processed for specified, explicit and legitimate purposes, and their processing is not incompatible with the purposes of the collection;

b the collected personal data are adequate, relevant and not excessive in relation to the purposes of the collection;

c personal data are not kept for longer than necessary for the purposes of the collecting or processing (and in compliance with CNPD deliberations);

d adequate technical and organisational measures are adopted to protect and secure the stored personal data;

e the data subject is provided information concerning the processing, as well as the right of access to rectify his or her personal data; and

f the CNPD has authorised (usually, for databases containing sensitive data) or has been notified of the processing prior to its commencement.

The data controller must also obtain prior unambiguous consent for the processing of personal data, except when the processing is necessary for certain specific purposes listed in the Data Protection Act.

Controllers must also provide data subjects with information containing:

a the identity of the controller and of his or her representative, if any;

b the purposes of the processing;

c the recipients or categories of recipients;

d whether replies are mandatory or voluntary, as well as the possible consequences of failure to reply; and

e the existence and conditions of the rights of access and rectification.

If data are collected through an open network, the data subject must be informed (except when he or she is already aware of the collection) that his or her data may be circulating on the network without security measures, and that the data may be at risk of being seen or used (or a combination of these) by unauthorised third parties.

Obligations of data processors

When the processing is carried out by a processor, the controller must enter into a written agreement with the processor with specific obligations:

a the processor must act only on the controller's instructions;

9 Personal data processing includes any operation or set of operations performed upon personal data, whether wholly or partly by automatic means, such as the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data.

b appropriate technical and organisational measures must be implemented by the processor as required by law to protect personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access, and all other unlawful forms of processing; and

c the data can only be processed on behalf of the controller and solely for the purposes agreed upon.

iii Technological innovation and privacy law

The CNPD has paid special attention to the challenges of technological innovation, in particular:

a radio-frequency identification (RFID): the controller must ensure transparent data collection and full data subject information on the use of RFID technology;

b use of geolocation and monitoring tracking technologies in the employment context: it is indispensable to ensure the right balance between adequate company management and employees' fundamental rights;

c automated profiling: online behavioural targeting requires explicit prior subject consent. The CNPD may authorise the processing of data if the processing is adequate and proportional and the data subjects' rights are not affected;

d electronic marketing: express prior consent is generally required. The CNPD is particularly attentive to this, since it is one of the most frequent causes for complaints;

e cookies: as a rule, prior express consent from the data subject is required, and he or she must have received clear and comprehensive information about the underlying purpose;

f drones: the use of drones poses special privacy concerns. In its Plan of Activities for 2016, the CNPD set the objective to contribute to new regulation on this matter, circumscribing the processing of personal data through those technologies and, whenever the processing takes place, circumscribing the notification exemptions; and

g internet of things (IoT): in its Plan of Activities for 2016, the CNPD set up a compromise to promote further investigation and education on the IoT's impact on privacy, considering it one of its priority thematic areas.

iv Specific regulatory areas

As stated above, the Data Protection Act is the primary legal source on data protection and, therefore, generally applies to any sector and area.

In any case, the privacy issues arising from the specific areas identified below are worth noting.

Employee monitoring

The CNPD published Opinion 7680/2014 setting out the conditions applicable to the processing of personal data regarding the use of geolocation technology in the workplace. In 2016, an interesting judicial decision from the Court of Appeal of Guimarães on the use of a global positioning system in a vehicle within a professional context was issued, ascertaining that the use of such devices to monitor the performance of the worker could be deemed remote surveillance and would not be admitted.

Electronic marketing

Under the ePrivacy Act, the delivery of unsolicited communications for direct marketing is subject to prior consent of the subscriber that is an individual or the user. An exception is made for pre-existing relationships: the supplier of a product or service may send advertising regarding its products and services to a client provided that the supplier has the client's contact details, and only if the advertisement pertains to the same products or services as those the client originally purchased. The client must explicitly be given the opportunity to object to such messaging at the moment of data collection and whenever a message is sent, and there must not be any charges for the recipient in addition to the telecommunication service cost.

Financial services

In addition to the Data Protection Act, specific security, bank secrecy and confidentiality obligations apply to financial services organisations. In August 2016, the CNPD issued an Opinion[10] on a legislative proposal to grant the Tax Authority access to bank account data. The proposal provided that Portuguese financial institutions should communicate the value of the deposits of all bank accounts to the Tax Authority. The CNPD considered this proposal illegal, and even unconstitutional. Furthermore, it considered the proposal contrary to the CJEU's previous decisions on banking secrecy.

IV INTERNATIONAL DATA TRANSFER

The Data Protection Act distinguishes transfers within the EU from transfers outside the region (to a third country).

Personal data may be freely transferred to another EU Member State, upon notification to the CNPD. In this case, data subjects must be informed if the data are transferred to a third party. For transfers outside the EU, the Data Protection Act distinguishes between countries with an adequate or inadequate level of data protection.

The transfer of personal data to a country that is not a member of the EU may only take place subject to compliance with the Data Protection Act and provided that the receiving country ensures an adequate level of protection.[11]

The rule is that a transfer of personal data to a country without an adequate level of protection may be allowed by the CNPD if the data subject has unambiguously consented to the proposed transfer (exceptions to this rule apply under the same terms of the 1995 Data Protection Directive).

The CNPD may authorise a transfer or set of transfers to a country that does not ensure an adequate level of protection if the data controller guarantees adequate data protection safeguards. This guarantee can be achieved through appropriate contractual clauses. Authorisation is granted by the CNPD under its own procedures and the decisions of the European Commission (which are typically followed by the CNPD on these matters).

The CNPD issued an opinion in 2004 that clarified the interpretation of Articles 19 and 20 of the Data Protection Act concerning transfers to countries outside the EU. With

10 As this Opinion has not yet been published, an identification reference is not available.

11 The adequacy of the level of protection of a country that is not a Member State of the EU is assessed in light of the circumstances surrounding a data transfer or set of transfers. It is for the CNPD or the European Commission to decide whether a country that is not a member of the EU ensures an adequate level of protection.

regard to data transfers to the United States, until the CJEU judgment in *Schrems v. Data Protection Commissioner* on 6 October 2015,[12] if a data importer based in the United States was self-certified regarding its adherence to the Safe Harbor Privacy Principles agreed between the EU and the US Department of Commerce, it was considered that the data exporter located in Portugal had the assurance that the company to whom the data were transferred had the adequate level of protection as required by the Data Protection Act.

Following the CJEU *Schrems* decision, the CNPD adopted, on 26 October 2015, a formal decision to issue only temporary authorisations for data transfers to the United States under the various alternatives to the Safe Harbor Privacy Principles, such as standard contractual clauses. Additionally, the CNPD decided to review all authorisations issued since 2000 concerning international data transfers under the Safe Harbor Privacy Principles and, in the meantime, decided that companies should promptly suspend all international data flows to the United States.

More recently, the European Commission adopted the Privacy Shield, a new framework aimed at protecting the personal data of EU citizens that are being transferred to the United States. The CNPD has not yet adopted specific procedures to deal with this new framework.

Nonetheless, whenever data are transferred to a data processor, the CNPD considers that the relationship between the data importer and the data exporter (the data controller) must also be ruled by a written agreement.

The European Commission decisions approving standard contractual clauses do not prevent national data protection authorities from authorising other contractual arrangements for the export of data out of the EU based on national law, as long as these authorities are satisfied that the contracts in question provide adequate protection for data privacy. The CNPD recognises the validity of other contractual arrangements for the export of data, provided that the contracts contain specific rules on data protection and comply with the requirements set by the Data Protection Act.

As to binding corporate rules, the CNPD does not accept the transfer of personal data based on unilateral declarations issued by multinational organisations or groups of companies. However, the CNPD has issued the Opinion 1770/2015 on the Intra-Group Agreements, providing that multilateral agreements between companies of the same group would be accepted as long as the data controller declares, in the data transfer notification, that the agreement is in accordance with the model clauses approved by the European Commission. The objective is to expedite the transfer of data outside the EU in these cases.

V COMPANY POLICIES AND PRACTICES

Data controllers may adopt several measures to improve their level of compliance with the data protection rules and reduce the risks associated with breaches of their obligations in this context. The GDPR will bring about a few significant changes to the current policies and practices, including new obligations and requirements. However, and for the time being, the current legislation lists the following measures to be implemented by data controllers.

12 CJEU Case C-362/14 (*Maximilian Schrems v. Data Protection Commissioner*).

i Compliance programmes

These programmes generally involve three phases: an audit of all data processing being carried out; definition of the actions required to assure compliance with the data protection law; and the implementation of measures allowing data controllers to have a 'full picture' of the relevant data protection matters in the context of their activity, and to provide them with the knowledge needed to manage data protection compliance.

ii Privacy officers

The appointment of a person responsible for data protection issues (the data privacy officer) is an important measure to assure compliance with the data protection obligations, notably in large organisations.

iii Regular audits

Regular audits are a determining factor for compliance with the Data Protection Act rules. It is fundamental for evaluating whether the purposes that determined the collection and the data storage periods, as well as the remaining data protection obligations, are being respected.

iv Privacy impact assessments (PIAs)

Without prejudice to overall continuous efforts to ensure compliance, PIAs should be carried out at the onset of a project with data processing operations. PIAs are an increasingly useful component of a privacy-by-design approach (i.e., where specific privacy features should be installed for specific operations, depending on the purpose and circumstances involved in each specific project). PIAs can reduce the risk of non-compliance, and are helpful in designing efficient processes for handling personal data.

v Data protection policies

Companies wishing to implement best practices regarding privacy matters should adopt specific policies and practices so as to comply with the Data Protection Act (e.g., an online privacy and cookies policy, data processing agreements, written consent and informative notices).

vi Security polices

Because of a real risk of loss and unauthorised disclosure of personal data, it is essential to adopt security policies with clear rules on the prevention of, and reaction to, a data breach situation.

VI DISCOVERY AND DISCLOSURE

The disclosure of personal data in response to national government requests varies significantly depending on the type of data requested.

For instance, disclosure of data collected in the context of the provision of electronic communication services is subject to the constitutional right to the confidentiality of private communications found in Article 34 Paragraph 1 of the Constitution. Furthermore, the Constitution prohibits government interference in private communications, with the only exception consisting in interference for criminal procedure purposes, in accordance with the applicable laws.

The Portuguese Criminal Code provides for the court-ordered interception of private communications in restricted circumstances. This interception can only take place for the purpose of investigating certain crimes.

Additionally, under Law 32/2008 of 18 July, providers of publicly available electronic communications services or of a public communications network must retain certain traffic and location data as well as certain data that allow for the identification of the subscriber or the user of the service. This data must be retained for one year from the date of the communication, and may only be accessed with a court order and for the purpose of the investigation, detection and prosecution of serious crime, as defined by Law 32/2008.

The CNPD Plan of Activities for 2016 sets up the analysis of legislation on data retention in the light of the CJEU decision on the invalidity of EU Directive 2006/24/EC as one of its top priorities.

With regard to foreign government requests, the same limitations apply: disclosure of communication data in response to these requests can only take place for criminal procedure purposes. The disclosure of other types of data is generally subject to the provisions regarding transfers of data to third entities. As expressly provided for in certain contexts, such as cybercrime or digital forensics for criminal investigation purposes (Law 109/2009 of 15 September), national authorities must cooperate with foreign authorities in accordance with the rules on data transfer to third countries.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The CNPD is responsible for supervising and monitoring compliance with data protection laws and regulations. Its enforcement powers include the authority to order the blocking, deletion or destruction of data, or the imposition of a temporary or permanent ban on the processing of personal data.

The CNPD actively investigates complaints received from individuals, and the number of inspections is growing significantly.

ii Recent enforcement cases

In line with its Plan of Activities to 2016, the CNPD has turned its attention on the marketing sector, and many recent enforcement actions have been related to direct marketing.

iii Private litigation

Data subjects may claim damages arising from the breach of their data protection rights before the civil courts.

Several decisions resulting from civil claims have focused increasingly on the privacy implications of new technologies, products and services, as well as social media. For instance, it has been deemed appropriate and proportional to impose on parents the duty to refrain from disseminating photos or information that allows the identification of their children on social networks so as to safeguard their right to privacy and the protection of their personal data and security in cyberspace.

In respect of personal data processing in social networks, it has been ruled that information shared through a group of friends on Facebook is considered public information

from the point of sharing onwards, and valid as evidence within disciplinary proceedings since, from this moment on, the personal data no longer enjoy proper protection under the right to confidentiality in communications.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The Data Protection Act is applicable to the processing of personal data where:

a the processing is carried out in the context of the activities of an establishment of the controller on Portuguese territory;[13]

b the controller is not established on Portuguese territory, but in a place where Portuguese law applies by virtue of international public law; or

c the controller is not established on EU territory and, for the purposes of processing personal data, makes use of equipment, automated or otherwise, situated on Portuguese territory, unless the equipment is only used for the purposes of transit through the territory of the EU.

Should the Data Protection Act apply to foreign organisations, the major compliance issues arise from international transfers (in particular, the fact that the CNPD does not recognise the validity of binding corporate rules), the information and consent rules, as well as the obligation to obtain the prior authorisation of the CNPD for certain data processing operations.

IX CYBERSECURITY AND DATA BREACHES

There is no general cybersecurity legislation in Portugal. However, there is legislation concerning the security of communication services and networks in the electronic communications sector. Entities providing publicly available electronic communications services in public communications networks must comply with Law 5/2004 of 10 February[14] (the Electronic Communications Law) and the ePrivacy Law. Under these laws, in the event of a security or integrity breach, these providers should notify the regulator (the National Communications Authority, or ANACOM),[15] the CNPD and, in some circumstances, service subscribers and users. In addition, more data breach notification obligations will apply in the future, with the application of the GDPR, since this legislation provides for notification to Data Protection Act obligations in all data breaches, independently of the sector in which these breaches occur.

The most important event in the context of cybersecurity in 2016 consisted of the approval of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the EU (the NIS Directive) on 6 July 2016. This Directive will allow the extension to other entities of the obligation to implement security measures and to notify security breaches. Along with the GDPR, the NIS Directive will definitely contribute to more robust information security. Member States must adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with the NIS Directive.

13 The CNPD generally considers that a PO box may be deemed an 'establishment' for the purposes of the Data Protection Act.

14 Amended by Decree-Law 176/2007, Law 35/2008, Decree-Law 123/2009, Decree-Law 258/2009, Law 46/2011, Law 51/2011, Law 10/2013, Law 42/2013, Decree-Law 35/2014 and Law 82-B/2014.

15 Formerly the Institute of Communications of Portugal, or ICP.

Regarding cybercrime, Portugal is a party to the Council of Europe's Convention on Cybercrime. Accordingly, the Portuguese criminal system protects confidentiality, integrity, availability and functionality of computer systems and of computer data. Almost all the provisions of the Convention on Cybercrime are transposed into the Portuguese legal system, mainly through the Cybercrime Act. The National Cyberspace Security Strategy, approved by Resolution of the Council of Ministers 36/2015 of 12 June, has set the road map for cybersecurity in Portugal for the next few years, setting up the main intervention axes for the National Cybersecurity Centre.

X OUTLOOK

The CNPD Plan of Activities for 2017 has been guiding its operations during the year, focusing on the evaluation of the Schengen Information System and the Visa Information System and, naturally, on the implementation of the GDPR in Portugal.

The CNPD's priority is to support the transition to the new legal framework enshrined in the GDPR, given that it will be fully applicable as of May 2018. For that purpose, the CNPD will have to prepare and reinforce its services to ensure the appropriate response to the new challenges arising from the GDPR, while struggling with a significant lack of human resources and funds. The CNPD has also undertaken to study the main changes introduced by the GDPR, contributing to the creation of a new legal framework for the protection of citizens' fundamental rights.

In January 2017, as indicated above, the CNPD approved and published a document establishing 10 measures to be taken by entities to prepare for the application of the GDPR. The CNPD has highlighted the main areas of intervention and set out some actions to be taken to ensure compliance with the new legislation. The CNPD will continue issuing guidelines on the GDPR with the purpose of ensuring that it is applied uniformly by the organisations affected.

Thus, we expect that active intervention and enforcement actions by the CNPD will increase in the future, with a growing impact on the way data protection is undertaken by data controllers. We believe that the adoption of the GDPR will also have a major impact on the level of awareness regarding data protection matters, and will influence the way data controllers 'shape' their compliance strategies.

Notably, in 2015 and 2016, the CNPD published the first issues of its electronic review, *Data Protection Forum*, which address some of the most recent and relevant topics on privacy and data protection.

On the subject of cybersecurity, the approval of the NIS Directive sets 9 May 2018 as the deadline for the adoption and publication of the new legislation, regulation and administrative provisions necessary to comply with this Directive. In 2016, the government conducted studies on cybersecurity and cyberdefence that will ultimately lead to further legislative developments in these areas.

In August 2017, the National Strategy of Security and Cyberspace was approved with the purpose of further developing network and information security, ensuring the defence and protection of critical infrastructure and vital information systems and enhancing a free, secure and efficient use of cyberspace by all citizens, and by companies and private and public entities.

Taking the above into consideration, given the profound shift in the legal framework that both the GDPR and the NIS Directive represent, it is expected that the immediate future will be very challenging for the government, the public and companies operating in relevant sectors, who must prepare themselves and adapt their procedures to ensure compliance with the new requirements that will be applicable in 2018.

Appendix 1

ABOUT THE AUTHORS

VDA VIEIRA DE ALMEIDA

Rua Dom Luis I, 28
1200-109 Lisboa
Portugal
Tel: +351 21 311 3400
Fax: +351 213113406
mpc@vda.pt
iab@vda.pt
www.vda.pt

MAGDA COCCO

VdA Vieira de Almeida

Magda Cocco is one of the partners in charge of the telecoms, media and IT practice, and is also head of the privacy, data protection and cybersecurity practice group. She has vast experience in the telecommunications sector in a variety of jurisdictions, with a special focus on Portuguese-speaking countries. In the data protection and cybersecurity sector, Magda has been involved in several public projects, providing expert advice both to private companies and public entities, and coordinating several compliance programmes in these areas.

INÊS ANTAS DE BARROS

VdA Vieira de Almeida

Inês Antas de Barros is a managing associate and an integral member of the telecoms, media and IT, privacy, data protection and cybersecurity practice group. Inês has been admitted as a legal expert to the European Privacy Seal. She has been involved in privacy compliance programmes and other privacy projects that raise complex issues across multiple jurisdictions and legal and regulatory areas (including health, pharmaceuticals, insurance, banking and telecommunications).

Strategic Research Sponsor of the
ABA Section of International Law

Law
Business
Research

ISBN 978-1-910813-89-8