The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 2
(published in November 2015 – editor Alan Charles Raul)

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor

Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, Felicity Bown, Joel Woods

ACCOUNT MANAGER
Jessica Parsons

PUBLISHING MANAGER
Lucy Brewer

MARKETING ASSISTANT
Rebecca Mogridge

EDITORIAL ASSISTANT
Sophie Arkell

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Robbie Kelly

SUBEDITOR
Gina Mete

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-75-2

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

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 INTERNATIONAL 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

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ADVOKATFIRMAET SIMONSEN VOGT WIIG AS

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K.

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JUN HE LAW OFFICES

LEE & KO

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

PEARL COHEN ZEDEK LATZER BARATZ

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 21

PORTUGAL

Magda Cocco, Inês Antas de Barros and Sofia de Vasconcelos Casimiro[1]

I OVERVIEW

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

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

Following the EU approach, Portugal has an omnibus data protection legal framework, which generally applies to both private and public sectors, as well as to any sector of activity (Data Protection Act, approved by Law No. 67/98 of 26 October 1998

1 Magda Cocco is a partner, Inês Antas de Barros is an associate and Sofia de Vasconcelos Casimiro is a consultant at Vieira de Almeida & Associados, RL.

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 entering into the home of any person without his or her consent except by order of the competent judicial authority and in the cases, and according to the forms, laid down by law. It also prohibits any interference with correspondence or telecommunications, apart from the cases laid down by law in connection with criminal procedure.

3 Article 35 provides that every citizen shall possess the right of access to all computerised data that concern him, 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.

(the Data Protection Act)).[4,5] Portugal has also approved Law No. 46/2012, of 29 August 2012 (the ePrivacy Act), concerning the processing of personal data and the protection of privacy in the electronic communications sector.[6]

The Portuguese Data Protection Authority (CNPD), the entity in charge of supervising the application of the regulations on data protection, was created in 1991. CNPD is an independent body with powers within the scope of the Assembly of the Republic, the national parliament.

Over the 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 the 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.

Recently 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 been contributing to awareness and to the creation of 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, CNPD has issued several opinions that received wide media attention.

In 2015, CNPD conducted an audit of the Portuguese Tax and Customs Authority following the creation of a 'VIP list' (a list concerning a special group of taxpayers composed of public figures linked to politics and sport).

The list was created to monitor unauthorised accessing of the data processes of those citizens, after several Treasury officials irregularly accessed and disclosed personal tax information of political figures (such as the Prime Minister and the President of the Republic) to third persons. CNPD concluded that no adequate security measures had been adopted and, therefore, data was made available to a broad spectrum of persons and confidentiality was compromised.

4 And amended by Law No. 103/2015 of 24 August 2015.

5 It transposes Directive 95/46/EC of the European Parliament and of the Council 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. 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.

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

Concerning the implementation of Foreign Account Tax Compliance Act reporting obligations, in 2014 CNPD issued a binding negative opinion on the agreement to be executed between the Portuguese and US governments, on the grounds that data protection obligations were not fully observed.

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

As to cybersecurity, in 2014 and 2015 several attacks on the information systems and websites of public entities were reported, with these attacks leading to defacement of websites and disclosure of confidential information. One such attack was perpetrated against the information system of the Attorney General's Office, which led to the disclosure of prosecutors' confidential information. In 2014, the National Cybersecurity Centre was created to secure nationally the management and use of information and communication technologies. Also in 2014, a Decree-Law creating the Cyberdefence Centre was enacted, providing for a decision centre within the armed forces for the development and coordination of cyberdefence capabilities. Implementation procedures for both centres continue in 2015.

In June 2015 the National Strategy for the Security of Cyberspace was enacted, setting the main principles for network and information security and proclaiming the strategic importance of cybersecurity and cyberdefence for Portugal.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

In Portugal, the legal data protection framework is regulated by: (1) Article 35 of the Constitution of the Portuguese Republic, (2) the Data Protection Act, (3) the ePrivacy Act; (3) and Law No. 32/2008, of 18 July, which sets out the data retention obligations imposed on providers of publicly available electronic communications services.[7] 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 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 liability 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).[8] 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

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

8 An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an indication number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

political beliefs, political party or trade union membership, religion, racial or ethnic origin, health or sex life, including genetic data, 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 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, the temporary or permanent prohibition of processing or publication of the judgment.

ii General obligations for data handlers

The Data Protection Act foresees a set of principles and obligations that data handlers must comply with when carrying out personal data processing,[9] with different status for controllers and processors.

Obligations of data controllers

The controller has extensive obligations. In particular, the controller is required to ensure that:

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

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

c personal data is not kept for longer than necessary for the purposes of the collecting or processing (and in compliance with CNPD's 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 CNPD has authorised (usually for databases containing sensitive data) or has been notified of the processing prior to its beginning.

The data controller must also obtain prior unambiguous consent for the processing of personal data, except when the processing is necessary to:

a the performance of a contract or contracts to which the data subject is party, or to take steps at the data subject's request before entering into a contract or a declaration of his or her will to negotiate;

b comply with a legal obligation to which the controller is subject;

9 Any operation or set of operations that is performed upon personal data, whether wholly or partly by automatic means, such as 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.

c protect the data subject's vital interests if he or she is physically or legally incapable of giving consent;
d perform a task carried out in the public interest or in the exercise of the official authority of the controller or of a third party to which the data is disclosed; and
e pursue the legitimate interests of the controller or of a third party to which the data is disclosed, except where those interests are overridden by the data subject's fundamental rights, freedoms and guarantees.

Controllers must also provide data subjects with information containing: the identity of the controller and of his or her representative, if any; the purposes of the processing; the recipients or categories of recipients; whether replies are mandatory or voluntary, as well as the possible consequences of failure to reply; and the existence and conditions of the right of access and rectification. If data is collected on an open network, the data subject must be informed, except when he or she is already aware, that his or her data may be circulating on the network without security measures and may be at risk of being seen and used 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: (1) the processor must act only on the controller's instructions; (2) appropriate technical and organisational measures must be implemented by the processor as required by law, to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing; and (3) the data can only be processed on behalf of the controller and solely for the purposes agreed.

iii Technological innovation and privacy law

CNPD has paid particular 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 and online behavioural targeting: this requires explicit prior subject consent. CNPD may authorise the processing of data if processing is adequate and proportional and data subjects' rights are not affected;
d electronic marketing: express prior consent is generally required. CNPD is particularly attentive to this, since it is one of the most frequent causes of 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; and
f drones: the use of drones poses special privacy concerns. In the absence of specific regulation on drones, CNPD has adopted a quite conservative approach.

iv Specific regulatory areas

As noted above, the Data Protection Act is the primary legislation regarding data protection and, therefore, generally applies to any sector and area.

Furthermore, the privacy issues arising from the specific areas identified below are worthy of note.

Employee monitoring

CNPD has published Opinion No. 7680/2014, setting out the conditions applicable to the processing of personal data regarding the use of geolocation technology in the workplace.

This opinion identifies obligations applicable to all companies and public entities dealing with geolocation data and sets out important rules for car manufacturers, car rental, leasing and fleet management companies, electronic communications operators, and all suppliers of platforms providing the necessary monitoring technology for geolocation devices.

CNPD has also issued Opinion No. 1638/2013 on the private use of electronic communications means in an employment context.

Electronic marketing

Under the ePrivacy Act, the delivery of unsolicited communications for direct marketing purposes, notably through automated calling and communication system without human intervention (automatic calling devices), facsimile machines (fax) or electronic mail, including SMS, EMS and MMS and other similar applications, is subject to the prior consent of the subscriber who 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 through having previously sold these products or services to the client, 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.

IV INTERNATIONAL DATA TRANSFER

The Data Protection Act distinguishes transfers within the European Union from transfers outside the region (third country).

Personal data may be freely transferred to another EU Member State, upon notification to 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.[10]

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

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 CNPD under its own procedures and the decisions of the European Commission (which are typically followed by CNPD on these matters).

CNPD issued an Opinion in 2004 in clarification of the interpretation of Articles 19 and 20 of the Data Protection Act concerning the transfer to countries outside the EU. This Opinion states that the transfer of personal data to those countries is allowed, and will not be subject to CNPD's prior authorisation, if: (1) there is a decision of the European Commission finding that a country offers an adequate level of protection; (2) any of the exemptions foreseen in Article 20 of the Data Protection Act is fulfilled; or (3) the transfers of personal data are made under the adoption of the standard contractual clauses approved by the European Commission.[11]

If a data importer that is based in the United States has self-certified its adherence to the Safe Harbor Privacy Principles agreed between the European Union and the US Department of Commerce, the data exporter located in Portugal has the assurance that the company to whom the data are transferred has the adequate level of protection as required by the Data Protection Act.

Nonetheless, whenever the data are transferred to a data processor, CNPD considers that the relation 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 authorising other contractual arrangements for the export of data out of the European Union based on national law, as long as these authorities are satisfied that the contracts in question provide adequate protection for data privacy. CNPD recognises the validity of other contractual arrangements for the export of data, provided that such contracts contain specific rules on data protection and comply with the requirements set by the Data Protection Act.

As to binding corporate rules, CNPD does not accept the transfer of personal data throughout multinational organisations or groups of companies.

---

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

11 Standard contractual clauses may not be amended, but the parties are free to include any other clauses on business-related issues provided they do not contradict the model clauses.

V COMPANY POLICIES AND PRACTICES

Data controllers may adopt several measures to improve their level of compliance with data protection rules and reduce the risks associated with breach of their obligations in this context.

i Compliance programmes

These programmes generally involve three phases: (1) an audit of all data processing being carried out, (2) definition of actions required to assure compliance with data protection law and (3) implementation of measures allowing data controllers to have a 'full picture' of the relevant data protection matters in the context of their activity and provide them with the knowledge needed to manage data protection compliance.

ii Privacy officers

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

iii Regular audits

Regular audits are a determining factor for compliance with Data Protection Act rules. It is fundamental to evaluate 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

Without prejudice to overall continuous efforts to ensure compliance, Privacy impact assessments (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., 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 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 respective 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 No. 32/2008, of 18 July, the 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 allows 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 No. 32/2008.

There is an interesting ongoing debate on the scope of the above-mentioned Article 34, Paragraph 4, of the Portuguese Constitution. This provision doesn't seem to expressly allow the government to interfere with any type of communications data for purposes other than criminal investigation. This has been disputed for some years. Several voices maintain that this limitation should be interpreted as referring exclusively to the content of communications, such as the conversation itself (in a voice communication such as a phone call), or the message itself (for written private communications). According to this interpretation, location or traffic data is not included in the scope of Article 34, Paragraph 4, and the government can process that type of data for any legitimate purpose.

This argument was put to the test in 2015, when the Portuguese Constitutional Court decided on whether a controversial bill, about to be promulgated by the President of Portugal, violated the Constitution, in particular, Article 34, Paragraph 4. The President referred the bill to the Constitutional Court because of doubts on the constitutionality of the provision granting the Portuguese information services access to traffic and location data for national security purposes, subject to prior authorisation by a commission composed of three Supreme Court of Justice judges.

On 27 August 2015, the Constitutional Court considered the bill incompatible with the Portuguese Constitution and, in particular, with the fundamental right to confidentiality in communications in Article 34, Paragraphs 1 and 4. The Court considered that both provisions include traffic data and location data and that the processing of communications data for national security purposes is not equivalent to processing for criminal procedure purposes, the former being merely preventive.

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 transfer of data to third entities. As expressly provided for in certain contexts, such as in cybercrime or in digital forensics for criminal investigation purposes (Law No. 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

CNPD is the entity responsible for supervising and monitoring compliance with data protection laws and regulations

CNPD's 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.

CNPD actively investigates complaints received from individuals and the number of inspections has been growing significantly.

ii Recent enforcement cases

One significant enforcement case that received media attention in Portugal, in 2014–2015, was the decision to apply to Optimus (an electronic communications services provider) a fine of €4,503,000 – reduced to €100,000 following two appeals – regarding the alleged infringement of the Data Protection Act and the ePrivacy Act.

iii Private litigation

Data subjects may claim damages arising from the breach of their data protection rights before 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 was 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 the right to privacy and the protection of personal data and security in cyberspace.

In respect of personal data processing on social networks, it was ruled that information shared through a group of friends on Facebook is considered public information from the point of sharing onwards, since from this moment on, the personal data no longer enjoys 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;[12]

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 European Union territory and, for the purposes of processing personal data, makes use of equipment, automated or otherwise, situated on Portuguese territory, unless such equipment is only used for purposes of transit through the territory of the European Union.

Should the Data Protection Act apply to foreign organisations, the major compliance issues arise from international transfers (in particular, the fact that CNPD does not recognise the validity of binding corporate rules), and information and consent rules, as well as from the obligation to obtain prior authorisation from 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 No. 5/2004, of 10 February[13] (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, ICP-ANACOM, CNPD and, in some circumstances, service subscribers and users.

Portugal is a state 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 provisions of the Convention on Cybercrime are transposed into the Portuguese legal order, mainly through the Cybercrime Act. In accordance with the action plan for the management and use of information and communication technologies, approved in 2012, the National Cybersecurity Centre was created (Decree-Law No. 69/2014, of 9 May). Although it plays an important role in the discussion of cybersecurity matters, as well as in the

12 CNPD tends to consider that a PO box may be deemed an 'establishment' for the purposes of the Data Protection Act.

13 Amended by Decree-Law No. 176/2007, Law No. 35/2008, Decree-Law No. 123/2009, Decree-Law No. 258/2009, Law No. 46/2011, Law No. 51/2011, Law No. 10/2013, Law No. 42/2013, Decree-Law No. 35/2014 and Law No. 82-B/2014.

awareness and in the support of many initiatives, its exact competences are still to be defined. This Centre must also coordinate with the recently created Cyberdefence Centre (Decree-Law No. 184/2014, of 29 December).

The National Strategy for the Security of Cyberspace, approved by Council of Ministers Resolution No. 36/2015, of 12 June, has set out the road map for cybersecurity in Portugal for the years to come.

X OUTLOOK

In the CNPD's published plan of activities for 2015/2016, which will guide its operations in the near future, it gives particular emphasis to conducting enforcement actions. One of the main areas of intervention will be unsolicited communications for direct-marketing purposes.

CNPD intends to analyse in deeper detail specific areas of interest, such as privacy in the electronic communications sector, cloud computing or smart cities, and drones.

Also in the pipeline is the issue of guidelines by CNPD on the use of cookies and fingerprinting devices.

It is, therefore, expected that active intervention and enforcement actions by CNPD will increase in the coming years, with a growing impact on the way data protection is taken into account by data controllers. We believe that the adoption of the EU's proposed new draft General Data Protection Regulation 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 strategy.

As to cybersecurity, there are expectations regarding the approval of the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high level of common network and information security across the Union (the Network and Information Security Directive). Alongside the General Data Protection Regulation, this Directive will allow the extension, to other entities, of the obligation to implement security measures and to notify security breaches. Although the exact scope of the Network and Information Security Directive is still to be defined, government and critical infrastructure companies are anticipating, and to some extent are already, preparing their procedures to comply with these new requirements.

Appendix 1

ABOUT THE AUTHORS

MAGDA COCCO

Vieira de Almeida & Associados, RL

Magda Cocco is a partner at Vieira de Almeida & Associados, RL and is in charge of the telecoms, media and IT practice, and she 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 compliance programmes in these areas.

INÊS ANTAS DE BARROS

Vieira de Almeida & Associados, RL

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

SOFIA DE VASCONCELOS CASIMIRO

Vieira de Almeida & Associados, RL

Sofia de Vasconcelos Casimiro is a consultant at Vieira de Almeida & Associados, RL and an integral member of the telecoms, media and IT, and privacy, data protection and cybersecurity practice groups. Sofia has vast experience on ICT issues and has been involved in landmark cases regarding P2P and other copyright matters, cybersecurity, cyberdefence, cybercrime and data protection. Sofia holds a doctorate and is a professor of law, teaching at Portugal's Military Academy and the European Defence Agency.

VIEIRA DE ALMEIDA & ASSOCIADOS, RL
Av. Duarte Pacheco, 26
1070-110 Lisbon
Portugal
Tel: +351 21 311 3400
Fax: +351 21 311 3406
mpc@vda.pt
iab@vda.pt
svc@vda.pt
www.vda.pt