The Privacy, Data Protection and Cybersecurity Law Review

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 1
(published in November 2014 – editor Alan Charles Raul).

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

The Privacy, Data Protection and Cybersecurity Law Review

Editor

Alan Charles Raul

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 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

www.TheLawReviews.co.uk

PUBLISHER
Gideon Roberton

BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, James Spearing

ACCOUNT MANAGER
Felicity Bown

PUBLISHING COORDINATOR
Lucy Brewer

MARKETING ASSISTANT
Dominique Destrée

EDITORIAL ASSISTANT
Shani Bans

HEAD OF PRODUCTION AND DISTRIBUTION
Adam Myers

PRODUCTION EDITOR
Timothy Beaver

SUBEDITOR
Janina Godowska

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 978-1-909830-28-8

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

ACKNOWLEDGEMENTS

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

ASTREA

BALLAS, PELECANOS & ASSOCIATES LPC

BOGSCH & PARTNERS LAW FIRM

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JONES DAY

KIM & CHANG

NNOVATION LLP

NOERR

PINHEIRO NETO ADVOGADOS

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SYNCH ADVOKAT AB

URÍA MENÉNDEZ ABOGADOS, SLP

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

EDITOR'S PREFACE

The first edition of *The Privacy, Data Protection and Cybersecurity Law Review* appears at a time of extraordinary policy change and practical challenge for this field of law and regulation. In the United States, massive data breaches have vied with Edward Snowden and foreign state-sponsored hacking to make the biggest impression on both policymakers and the public. In Europe, the 'right to be forgotten', the draconian new penalties proposed in the draft Data Protection Regulation and the Snowden leaks, have significantly altered the policy landscape.

Moreover, the frenetic conversion of the global economy to an increasingly digital, internet-driven model is also stimulating a rapid change in privacy, data protection and cybersecurity laws and regulations. Governments are playing catch-up with technological innovation. It is reported that half the world's population will be online by 2016 and the economies of emerging nations (except, perhaps, in Africa) are being developed directly through electronic commerce rather than taking the intermediate step of industrial growth as Western economies did. Growth and change in this area is accelerating, and rapid changes in law and policy are to be expected.

In France, whistle-blowing hotlines are meticulously regulated, but now, in certain key areas like financial fraud or corruption, advance authorisation for the hotlines is automatic under a 2014 legal amendment. In Singapore, 2014 saw the first enforcement matter under that country's Personal Data Protection Act – imposing a financial penalty on a company that sent unsolicited telemarketing messages. In Russia, a new 2014 'forced localisation' law requires data about Russians to be stored on servers in-country rather than wherever the data can be most efficiently managed and processed, and jurisdictions around the world have debated enacting such proposals. Interestingly, while notice of the location of the relevant servers must be provided to the Russian data protection authority, it is not clear whether the law prohibits personal data to be simultaneously stored both in-country and in foreign servers.

The European Union continues to seek to extend its model for data protection regulation around the world by deeming only countries that adopt the 'omnibus' legislative approach of the EU to be 'adequate' for data protection purposes. The EU model is not being universally endorsed, even outside the US and the Asia and Pacific

Economic Cooperation (APEC) economies. But nonetheless, the EU's constraints on international data transfers have substantially inhibited the ability of multinational companies to move personal data around the world efficiently for business purposes. In particular, conflicts with the US abound, exacerbated by the Snowden leaks regarding US government surveillance. One of the primary methods by which such EU–US data flows are facilitated, the US–EU Safe Harbor regime, has come under attack from EU parliamentarians who believe that such information will not be as carefully protected in the US and could become more susceptible to surveillance, despite the comparable surveillance authorities of EU intelligence agencies.

While policy conflicts over data protection conflicts appeared to be moderating before the Snowden leaks, afterwards, officials around the world professed to be so shocked that governments were conducting surveillance against possible terrorists that they appear to have decided that US consumer companies should pay the price. Some observers believe that digital trade protection, and the desire to promote regional or national 'clouds', play some role in the antagonism leveled against US internet and technology companies.

The fact that the US does not have an omnibus data protection law, and thus does not have a top-level privacy regulator or coordinator, means that it has been difficult for the US to explain and advocate for its approach to protecting personal information. This has allowed the EU to fill a perceived policy void by denying mutual recognition to US practices, and to impose significant extraterritorial regulatory constraints on American and other non-European businesses.

Nevertheless, it cannot be denied that privacy enforcement in the US is distinctly more aggressive and punitive than anywhere else in the world, including the EU. Substantial investigations and financial recoveries have been conducted and achieved by the Federal Trade Commission (which has comprehensive jurisdiction over consumer data and business practices), 50 state attorneys general (who have even broader jurisdiction over consumer protection and business acts and practices), private class action lawyers who can bring broad legal suits in federal and state courts, and a plethora of other federal and state agencies, such as the Consumer Financial Protection Bureau, the Federal Communications Commission, the Department of Health and Human Services (for medical and health-care data), the Department of Education, the Securities and Exchange Commission and various banking and insurance agencies.

In sum, there are no shortage of privacy regulators and enforcers in the US, Europe, and Asia. Enforcement in South America, as well as Africa and the Middle East appears to be developing more slowly.

Trumping many other privacy concerns, however, is the spate of data breaches and hacking that have been epidemic and part of public discourse in the years following California's enactment of the first data breach notification law in 2003. While the US appears (as a consequence of mandatory reporting) to be suffering the bulk of major cyberattacks – on retailers, financial institutions and companies with intellectual property worth stealing by foreign competitors or governments – it is also true that the US is leading the rest of the world on data breach notification laws and laws requiring that companies adopt affirmative data security safeguards for personal information.

For corporate and critical infrastructure networks and databases, the US has also led the way with a presidential executive order and the Cybersecurity Framework

developed by the National Institute of Standards and Technology in the US Department of Commerce. The United Kingdom has also been a leader in this area, developing the UK CyberEssentials programme, which will soon include an option for companies to be certified as compliant with the programme's cybersecurity standards. The EU Parliament has also enacted cybersecurity directives, and the EU's European Network and Information Security Agency has provided extensive and expert analysis, guidance and recommendations for promoting cybersecurity for EU-based organisations.

Despite attempts to implement baselines for cyber safeguards, it appears that no one is immune and no organisation is sufficiently protected to have any confidence that it can avoid being the victim of successful cyberattacks, particularly by the sophisticated hackers employed by state sponsors, organised crime, social hacktivists or determined, renegade insiders (like Snowden). Government agencies and highly resourced private companies have been unable to prevent their networks from being penetrated, and sometimes are likely to identify 'advanced persistent threats' months after the malware has begun executing its malicious purposes. This phenomenally destructive situation cannot obtain, and presumably some more effective solutions will have to be identified, developed and implemented. What those remedies will be, however, is not at all clear as 2014 yields to 2015.

In the coming year, it would seem plausible that there could be efforts at international cooperation on cybersecurity as well as cross-border enforcement against privacy violators. Enforcers in the EU, US and among the APEC economies, may increasingly agree to work together to promote the shared values embodied in the 'fair information practices principles' that are common to most national privacy regimes. In early 2014, a step in this direction was taken when APEC and the European Union's Article 29 Working Party (on Data Protection) jointly released a framework by which international data transfers could be effectuated pursuant to the guidelines of both organisations.

Challenges and conflicts will continue to be factors with respect to: assurances of privacy protection 'in the cloud'; common understandings of limits on and transparency of government access to personal data stored either in the cloud, or by internet companies and service providers; differences about how and when information can be collected in Europe (and perhaps some other countries) and transmitted to the US for civil discovery and law enforcement or regulatory purposes; freedom of expression for internet posts and publications; the ability of companies to market on the internet and to track – and profile – users online through cookies and other persistent identifiers; and the deployment of drones for commercial and governmental data acquisition purposes.

The biggest looming issue of them all, however, will likely be 'big data'. This is a highly promising practice – based on data science and analytics – that collects and uses enormous quantities of disparate (and often unstructured) data, and applies creative new algorithms enabled by vastly cheaper and more powerful computer power and storage. Big data can discover helpful new patterns and make useful new predictions about health problems, civic needs, commercial efficiencies, and yes, consumer interests and preferences.

The potential social utility of big data has been unequivocally acknowledged by the US administration as well as by the key policymakers in the EU. But, big data challenges the existing privacy paradigm of notice and disclosure to individuals who are then free to

make choices about how and when their data can be used and collected. Many existing and proposed applications of big data only work if the vast stores of data collected by today's companies can be maintained and analysed irrespective of purpose limitations. Such limitations may have been relevant (and disclosed) at the point of collection, but no longer address the value of the data to companies and consumers who can benefit from big data applications. Numerous highly thoughtful reports by policymakers in the US and EU have noted concerns about the possibility that unfettered big data applications could result in hidden discrimination against certain demographic groups that might be difficult to identify and correct; or could result in undue profiling of individuals that might inhibit their autonomy, limit their financial, employment, insurance or even serendipitous choices, or possibly somehow encroach on their personal privacy (to the extent that otherwise aggregate or anonymous data can be re-identified).

This publication arrives at a time of enormous ferment for privacy, data protection and cybersecurity. Readers are invited to provide any suggestions for the next edition of this compendium, and we look forward to seeing how the many fascinating and consequential issues addressed here will evolve or develop in the next year.

Alan Charles Raul
Sidley Austin LLP
Washington, DC
November 2014

Chapter 8

GREECE

George Ballas and Theodore Konstantakopoulos[1]

I OVERVIEW

The Greek Constitution provides the backbone of the protection of personal data in Greece, establishing, at the highest level, a personal right aiming at the protection of individuals from the collection and processing, especially by electronic means, of their personal data. Data privacy is a matter of further horizontal and also sector-specific regulation, which implements relevant EU data protection legislation.

Despite the absence of particularly active NGOs and self-regulating industry groups in the field of data privacy, data protection issues have, nevertheless, over the past few years, gradually gained increased media coverage and are now often included in the political agenda. Recent major data breach incidents in Greece and the impact of the NSA scandal (the Snowden case), along with fact that the Greek regulator, the Hellenic Data Protection Authority (DPA) and the Cyber Crime Unit of the Hellenic Police are actively engaged in pursuing non-compliance, have raised public awareness of privacy and security issues.

II THE YEAR IN REVIEW

Recent data breaches and the action taken by the competent authorities in response are indicative of the data privacy risks especially in a digitally connected world.

Public attention was placed on data leak cases, with most important being a data leak from the Greek Ministry of Finance; a man was arrested for unlawful possession of personal data of 9 million Greek people (representing more than 80 per cent of Greece's population). Moreover, a fine was imposed on a major music label for failure

1 George Ballas is the senior partner and Theodore Konstantakopoulos is an associate at Ballas, Pelecanos & Associates LPC.

to implement appropriate organisational and technical measures; the company's website was hacked and the personal data of 8,385 subscribers and clients were leaked.

In this context, on-site audits by the competent authorities have been focusing on data security issues; the DPA in the framework of an annual programme of regular audits in the field of e-government, reviewed the IT systems 'e-School' and 'e-Datacentre' of the Ministry of Education and ordered the implementation of appropriate security measures.

Also noteworthy is a fine imposed by the DPA on a newspaper website for the publishing of sensitive personal data relating to a criminal prosecution. The regulator noted that such web publishing can disproportionately affect the rights of individuals, because it can lead to free, universal and uncontrolled access to such information via search engines without any time limitation.

Recent developments include the DPA's Decision 136/2013 on Google Street View, which gave the green light for the provision of the service. The service was initially blocked by the DPA in 2009 due to concerns about data privacy. According to the Decision, Google must blur out the faces and licence plates of cars, while there will be a tool in place, which can be used by users in order to request such blurring, including blurring of house facades. Moreover, Google must inform the data subjects via the press and its website about the data processing in question.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Article 9(a) of the Greek Constitution establishes, at the highest level, a personal right aiming at the protection of individuals from the collection and processing, especially by electronic means, of their personal data. This provision is also the legal foundation of the establishment of the DPA.

The legislative framework for the protection of personal data includes the Data Protection Law 2,472/1997 on the Protection of Individuals with Regard to the Processing of Personal Data (DPL) and Law 3471/2006 on the Protection of Personal Data And Privacy In The Electronic Telecommunications Sector (PECL), which implement the relevant EU data protection legislation (Directives 95/46/EC and 2002/58/EC).

Other sector-specific data privacy regulation in place is, for instance, Law 3,917/2011 (implementing Data Retention Directive 2006/24/EC), applicable to providers of publicly available electronic communication services or of public communication networks, providing for specific data retention requirements.

It is noted that the Greek legal framework also includes guidelines issued by the DPA and published on its website (e.g., guidelines on spam, health data, internet services, new technologies and social security data) and directives also issued by the DPA (such as Directive 50/2001 on Direct Marketing, Directive 115/2001 on Privacy at Work, Directive 1/2005 on Data Deletion, Directive 1/2011 on the Use of CCTV and Directive 2/2011 on Electronic Consent).

Key terms in this field are the 'data subject', namely, the individual who is the subject of personal data, the 'data controller', namely, the person (including individuals, legal entities and state authorities) who determines the purposes for which and the

manner in which personal data are processed, and the 'data processor', namely, the person who processes the personal data on behalf of the data controller.

The sanctions envisaged by the DPL and imposed by the DPA for breach of the DPL provisions depend on the severity and the particular circumstances of each case. Administrative sanctions include: warning letters with an order for the violation to cease within a specified time limit; fines ranging from €880 to €146,735 (further to a hearing); temporary or definitive revocation of a permit previously issued by the DPA (further to a hearing); orders for the destruction of the data file; or ban a on any further data processing (further to a hearing). Criminal sanctions provided by the DPL include imprisonment of up to five years, fines, or both. Damages claims by data subjects are also possible; however, the actual existence of damage will often be difficult to prove. It is noted that in such case a court could also award compensation for (non-pecuniary) moral damage suffered by the data subject.

ii General obligations for data handlers

The general principle introduced by the DPL is that personal data, to be lawfully processed, must be: (1) collected fairly and lawfully for specific, explicit and legitimate purposes and be fairly and lawfully processed in view of such purposes; (2) adequate, relevant and not excessive in relation to the purposes for which they are processed at any given time; (3) accurate and, where necessary, kept up to date; and (4) stored in a form that permits the identification of data subjects for no longer than the period required for the purposes for which the data was collected or processed.

The processing of personal data is in principle permitted only when the data subject has provided his or her consent. Exceptions apply; for instance, when processing is necessary for the execution of a contract to which the data subject is party, no consent is required (provided that the data subject has been properly informed), or when data processing involves clients' or suppliers' personal data, provided that such data are neither transferred nor disclosed to third parties.

The collection and processing of sensitive data is prohibited. The DPL defines 'sensitive data' as data referring to racial or ethnic origin, health, sexual life and social welfare. Exceptionally, collection and processing of sensitive data may be permitted by virtue of a permit issued by the DPA, under specific conditions, such as when the data subject has provided his or her written consent, or when processing is carried out exclusively for research and scientific purposes, provided that anonymity is ensured and all necessary measures for the protection of the persons involved are taken, or when processing is carried out by a public authority and it is necessary for the purposes of national security, protection of public health, tax enforcement or it pertains to the detection of offences.

At the data collection stage, the data subject must be informed, at least, of: the identity of the data controller and its representative (if any); the purpose of data processing; the recipients or the categories of recipients of the data; and the existence of a right to access and object.

Data subjects have the right to access the personal data relating to them and being processed by the data controller; the data subject can request and obtain from the data controller, without undue delay and in an intelligible and express manner, information

about the nature of such personal data, their origin, the purposes of processing and the recipients, if any, thereof. Data subjects also have the right to object to the processing of their personal data by sending a notice to the data controller, including a request for a specific action, such as correction, temporary non-use, non-transfer or deletion.

According to the DPL, the data controller must notify the DPA in writing about the establishment and operation of a file or database or the commencement of data processing (exceptions apply).

iii Technological innovation and privacy law

The implementation of new technologies for the needs of behavioural advertising and also in the workplace poses new data privacy and security challenges.

The use of cookies is regulated in Greece by Article 170 of Law 4,070/2012 (implementing the EU Cookies Directive (2009/136/EC) and amending Article 4 of PECL), which provides that the storage of information on or the access to information already stored on a device is permitted only if the user of the device has provided informed consent. Such consent can be expressed by using the appropriate settings of a browser or other application. The above does not prevent any technical storage or access for the sole purpose of carrying out a transmission of a communication over an electronic communications network or any technical storage or access that is necessary for the provision of an information society service, which has been explicitly requested by the user.

The recently published DPA Guidelines on Cookies attempt to further explain the relevant provision. They refer to exceptions where no consent is required (basically reproducing the Article 29 Working Party Opinion 04/2012 on Cookie Consent Exemption). These exceptions are: 'user-input' cookies, user-centric security cookies, multimedia player session cookies, authentication cookies, user interface customisation cookies, load-balancing session cookies and social plug-in content-sharing cookies. Special reference is also made to web analytics cookies and online advertising cookies (first and third-party cookies), which according to the DPA Guidelines are not included in the above exceptions and therefore prior consent is required. Nevertheless, the DPA recognises the need to further review and discuss the issue of web analytics cookies. It is also noted that a user-friendly mechanism to opt out must be in place.

While the implementation of internet of things technologies has not yet been officially regulated in Greece, geolocation and radio frequency identification (RFID) technologies have been within the scope of the DPA's mission and work and are often an issue of legal debate.

The DPA has adopted the Article 29 Working Party Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications. Even before its publication, the DPA, in line with the Working Party's opinion, in 2007 had listed the protection measures that should support the use of RFID technology, suggesting the use of privacy enhancing technologies, privacy and security policies, certification of the data processors, access controls, maintenance of activity logs, data breach management systems, the implementation of cryptographic technologies and protocols, anonymity, unlinkability and unobservability.

Moreover, the DPA has in its Decision 112/2012 addressed the issue of the use of geolocation technology for the location tracking of individuals (e.g., minors or patients) with the possibility of an alarm button. Such technology may involve the collection and processing of sensitive personal data and data transfers outside the EU/EEA (especially in conjunction with the advancing use of cloud technology). Although the Decision focuses mainly on GPS and GSM technologies, its conclusions with regard to legitimate ground, information and data subject's rights could also apply to internet of things technologies (RFID chips, barcodes, etc.). The DPA highlights in particular the data controller's obligation to provide adequate information to data subjects about the data collection and processing in question (and obtain the data subject's informed consent, when required) and the data controller's obligation to implement appropriate organisational and technical data security measures, imposing, for example, the use of cryptography, physical security measures, verification and identification mechanisms and the use of eight-character passwords.

The use of geolocation systems has also been examined by the DPA in the context of privacy at work (DPA Directive 115/2001).

The increasing use of profiling facilitated by new technologies (mobile apps, big data, etc.) falls within the scope of the DPL. A data subject is entitled to request from the competent court the immediate suspension or non-application of a decision affecting him and which is based solely on automated processing of data intended to evaluate his or her personality and especially his or her performance at work, creditworthiness, reliability and general conduct. The current legal framework does not prevent the creation of profiles on individuals, but it ensures that individuals will not be the subject of automated decisions based on such profiling that could have negative consequences for their lives.

The DPA, applying the above provision to employment relationships, concluded in its Directive 115/2001 on privacy at work (the Privacy at Work Directive),[2] that decisions regarding every aspect of the personality of employees may not be taken solely based on automated processing of their personal data as this would turn the employees into data objects and would insult their personality. This means that the evaluation of employees' productivity should include human assessment and should not be based solely on statistics and data aggregated by the automated processing of data.

iv Specific regulatory areas

Electronic marketing

Electronic communication by e-mail and SMS for direct marketing purposes requires the recipient's consent (opt-in). An exception applies when the contact details of the recipient have been lawfully obtained in the context of the sale of a product or a service. In that case, e-mails and SMS can be sent for direct marketing of similar products or services even when the recipient of the message has not provided prior consent, provided

2 Based on the Article 29 Working Party working document 55/2002 on the surveillance of electronic communications in the workplace.

that he or she is clearly and distinctly given the option to object, in an easy manner and free of charge, to such collection and use of electronic contact details.

Health data

Apart from the DPL, with regard to health data, the Medical Ethics Code (Law 3,418/2005), Law 2,071/1992 on the national health system and Article 371 of the Greek Penal Code apply, according to which medical professionals must keep their patients' medical data confidential. DPA Decisions 33/2007 and 43/2011 placed significant emphasis on the organisational and technical measures that a data controller (in these cases, the Ministry of Justice and a public hospital, respectively) needs to implement, especially when sensitive health data is being collected and processed. The recent DPA Decision 46/2011 dealt with the issue of medical data transfer from one insurance company to another. The transfer was not prohibited *per se*, but it was only permitted under strict circumstances (e.g., the patient needs to be properly informed and the DPA needs to issue a permit, as applicable in each case).

The European Committee for Standardization (CEN), of which Greece is a member, has established Technical Committee 251 (TC 251), a working group on standardisation in the field of health information. The CEN standards are further adopted by the Hellenic Organisation for Standardisation (ELOT). However, until the adopted standards are included in some form of legislation, they are non-binding and are followed on a voluntary basis.

Employee monitoring

According to the Privacy at Work Directive, the collection and processing of employees' communication data (e.g., e-mails and call logs) is permitted only if this is absolutely necessary for the performance of the assigned work or for general management purposes (e.g., communication costs management). Collection and processing of data regarding incoming and outgoing calls and communications in general (e-mails are included) in the workplace is again allowed, as long as processing is absolutely necessary in order to control the employees' performance and for business organisation purposes, e.g. for expenditure control. Such data must be limited to what is absolutely necessary and appropriate to achieve the data collection purposes. Access to the full communication numbers or to the content of such communications, including the real-time remote monitoring of employee communications and activity is not permitted for the above purposes, unless there is a permit by a judicial authority in place.

Moreover, collection and processing of personal data regarding the web activity of employees must be based on the principle of purpose and proportionality and it may only be permitted when there is a need to control a behaviour prohibited by law, the employment agreement or regulations, or behaviour in breach of a code of conduct, such as visiting websites with pornographic content.

The general, the systematic and proactive collection and processing of such data is not permitted. In all cases the employees need to be informed about such collection and processing or about the possibility of such collection and processing if they act in breach of the applicable laws and regulations, their employment agreement or employer's code of conduct. This notification must be specific and detailed, and ideally it should take place before the commencement of the employment relationship.

Debt collection agencies

Due to the current financial distress, the regulation of debt collection agencies has become an issue of special interest in Greece. According to Law 3,758/2009 on Debt Collection Agencies, as amended by Law 4,038/2012 and currently in force, before a creditor involves a debt collection agency, the creditor must inform the debtor about the former's right to transfer the latter's personal data to debt collection agencies. The creditor's consent is not required for such a transfer.

According to the relevant DPA guidelines, the notification of a debtor can take place either by the general agreement between the parties or, at least, via the last written notice by the creditor to the debtor, urging the latter to settle his or her outstanding debt. The notice can also be included in a separate letter or in the debit notes (always before the the involvement of a debt collection agency). According to the DPL and DPA Decision Γ/ΕΞ/4744 of 12 July 2013, such notice to debtor must include the identity of the data controller; the pufpose for data processing (i.e., debt collection within the scope of Law 3,758/2009); the recipients of such data (i.e., debt collection agencies – reference to specific debt collection agencies is not required); and the debtor's rights to access and object.

IV INTERNATIONAL DATA TRANSFER

As a general rule, the transfer of personal data is permitted within the Member States of the European Union (EU) and the European Economic Area (EEA); personal data can only be transferred to countries outside the EU/EEA when an adequate level of protection is guaranteed.

Under the DPL, the DPA is responsible for determining whether a country that is not a Member State of the EU or EEA guarantees an adequate level of protection and for granting permits for data transfers to that country.

A permit by the DPA is not required if the European Commission has decided, on the basis of the process of Article 31, Paragraph 2 of Directive 95/46/EC, that the country in question guarantees an adequate level of protection within the meaning of Article 25 of the Directive. The transfer of personal data to a non-Member State that does not ensure an adequate level of protection is exceptionally allowed only following a permit granted by the DPA and provided that specific conditions occur (the data subject's consent, data transfer contractual clauses, etc.). No permit is required when standard contractual clauses (model clauses) or binding corporate rules are in place.

V COMPANY POLICIES AND PRACTICES

According to the DPL, the processing of personal data must be confidential. It must be carried out solely and exclusively by persons acting under the authority and instructions of the data controller. In order to carry out data processing data controllers and data processors must choose persons with professional qualifications that provide sufficient guarantees in respect of technical expertise and personal integrity in order to ensure such confidentiality and must also implement appropriate organisational and technical measures to secure data.

If data processing is carried out by a data processor on behalf of the data controller, such assignment must be in writing and provide that data processor carries out the data processing pursuant to the instructions of the data controller and that all security obligations imposed by law on the data controller shall also be borne by the data processor.

Further, the DPA Directive 1/2005 on Data Deletion refers to specific 'secure' deletion methods and procedures. Also relevant are the DPA Guidelines on Security Policy, Security Plans and Disaster Recovery and Contingency Plans, which are published and available on the authority's website.

In the private sector the appointment of a data privacy officer is not mandatory although it is considered best practice. In contrast, the providers of public communication networks or public electronic communication services in the context of their data retention obligations imposed by Law 3,917/2011 (implementing Directive 2006/24/EC) must appoint a data security officer (DPA and ADAE Joint Act 1/2013). For public sector entities offering e-governance services, the appointment of a data protection officer is obligatory by virtue of Law 3,979/2011, according to which the data protection officer is responsible for the implementation of technical and organisational measures to ensure compliance with the principles and obligations provided by the data privacy legislation and also for the drafting of a privacy and security policy and for the provision of data privacy policy training to employees and personnel.

As matter of best practice, a data protection officer would be expected to have a detailed and up-to-date knowledge of the data collection and processing operations of the organisation, to identify the scope, the purposes and the means of each data processing operation and to maintain a list of all personal sdata databases or files. A data protection officer is expected to proactively identify policy issues, conduct internal reviews, draft internal reports and generally observe any legal data protection obligations.

Moreover, it is noted that according to Law 1,767/1988 (regulating workers' councils), workers' councils jointly decide with the employer, *inter alia*, the means of monitoring of the employees' presence and behaviour in the workplace, in particular regarding the use of audiovisual means for such purpose. The parties' agreement on this issue must be in writing.

VI DISCOVERY AND DISCLOSURE

i Consent and warrants

The general principle, as outlined in the DPL, is that processing of personal data (including access to such data) is permitted only when the data subject has provided his consent. Exceptionally, personal data can be processed without the data subject's consent, when, *inter alia*, processing is necessary 'for the performance of a task of public interest or of a task carried out by a public authority in the framework of the exercise of its authority'. In particular with regard to sensitive data, collection and processing of such data is prohibited. Exceptionally, collection and processing of 'sensitive data' can take place pursuant to a warrant issued by the DPA, when, *inter alia*, 'processing is carried out by a public authority and is necessary for the purposes of national security; criminal or punishment policy and pertains to the detection of offences, criminal convictions or

security measures; the protection of public health; or the exercise of public control on tax or social services.

No warrant will be required when processing is carried out by judicial authorities. Indeed, more generally the DPL provisions do not apply to the processing of personal data carried out by the judicial authorities, the Public Prosecutor's Office and by the authorities acting under their supervision, in the framework of their duties and in order to investigate crimes punished as felonies or misdemeanours (with *dolus*). In the case of such processing, legislation regarding the lifting of the constitutional right to private communications will be applicable (see subsection iii, *infra*).

ii Cross-border data transfer

According to the DPL, cross-border data transfer can be allowed on the basis of a DPA warrant, provided that 'the transfer is necessary for the establishment, exercise or defence of legal claims in court' implementing Article 26(1)(d) of Directive 95/46/EC. The Directive does not, however, require the establishment, exercise or defence of legal claims to take place in a specific forum, while the Greek transposition (the DPL) adopts a stricter approach and does require a court proceeding. Hence, it is questionable whether the exception in question will also cover pretrial disclosure proceedings.

Moreover, reference is also made to the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Evidence Convention). Greece is a party to the Hague Evidence Convention, which permits evidence to be transmitted to other countries via a 'letters of request'. The court where the action is pending issues the letters to the 'central authority' of the jurisdiction where the discovery is located, which then forwards the letters to the domestic judicial authorities competent to execute them.

Further to the above, a legal tool also available to law enforcement agencies are disclosure requests made on the basis of mutual legal assistance treaties (MLAT), which allow generally for the exchange of admissible evidence and information in criminal matters. There has been a US–EU MLAT in force since 2003, which applies in relation to MLATs between the EU Member States and the US that were already in force. Greece and the US have signed a MLAT, which has been in force since 20 November 2001, which covers assistance in connection with the investigation, prosecution and prevention of offences and in proceedings related to criminal matters (such as organised crime and murder). Such assistance includes providing documents and records; locating or identifying persons or items; and executing searches and seizures.

iii The right to private communication

As regards surveillance and government access to data, the Greek Constitution establishes the 'absolute inviolability' of the privacy or secrecy of communication, which can be side stepped only for very specific cases (national security and a very limited number of felonies, including forgery, bribery, murder, robbery, and extortion) and only under the guarantees and supervision of the judiciary and the involvement of a constitutionally established independent authority (with the sole purpose of safeguarding the confidentiality and secrecy of communications).

The 'lifting of secrecy' applies only to communication conducted via communication networks or via communication service providers. The types and forms

of communication that are subject to the lifting of secrecy are, *inter alia*, telephone (fixed and mobile), data communication via data networks, internet communication, wireless communication, satellite communication, and services provided in the framework of the above forms (e.g., automatic answering machines, SMS/MMS, access to websites, access to databases, e-mail, electronic transactions, directory information and emergency services).

A list of the felonies for which the right to privacy can be waived can be ordered and the procedures, time limits and technical and organisational safeguards that need to be followed are analysed in Law 2,225/1994 and Presidential Decree 47/2005. Only the competent public prosecutor or a judicial authority or other political, military or police public authority, competent for an issue of national security requiring the lifting of the right to privacy, may submit a request to that effect, which then can be ordered by the appeals prosecutor or the competent judicial council (exceptionally by the public prosecutor).

The Hellenic Authority for Communication Security and Privacy (ADAE) reviews such judicial orders and monitors compliance with the conditions and the procedures for waiving the right to privacy. From a practical perspective and according to the 2013 Annual Report of the ADAE, in 2013 the authority received and reviewed 4,141 prosecutor's orders regarding lifting the right to privacy for national security issues (a significant increase from the figure of 2,634 in 2012); 5,006 requests for the extension of already issued prosecutor's orders (an increase from 3,913 in 2012); and 2,334 judicial council orders regarding the lifting of of the right to privacy in relation to serious felonies (increased from 2,055 in 2012).

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The DPA, a constitutionally established and independent authority is responsible for overseeing the data protection law in Greece. The DPA issues regulatory acts for the purpose of a uniform application of the data protection legislation, publishes guidelines, addresses recommendations and instructions to data controllers, grants warrants for the collection and processing of sensitive data and for the cross-border flow of personal data, imposes administrative sanctions and performs administrative audits.

On-site audits by the DPA can be *ex officio* or in response to complaints. Such regulatory audits are quite common and often lead to administrative sanctions. In 2013 the DPA examined 692 complaints and performed 10 audits on nine data controllers. In order to review compliance with applicable data privacy legislation, private companies cooperated with the Cyber Crime Unit of the Hellenic Police, issued warning letters with an order for compliance and imposed fines in 20 cases (adding up to a total of €315,000).

The ADAE, a constitutionally consolidated independent authority, is responsible for protecting the secrecy of communication and the security of networks and information. The ADAE can conduct on-site audits to review compliance with the Regulation for the Safety and Integrity of Networks and Electronic Communications Services. Depending on the severity and the particular circumstances of each case, the

ADAE can issue warning letters with an order for compliance and impose fines ranging from €15,000 to €1.5 million.

In 2013 the ADAE performed ordinary audits of four providers of electronic communication services; 22 extraordinary audits of 11 such providers; and audits of two public authorities (namely, the Hellenic Police and the National Intelligence Service) and the Greek Parliament in order to examine the legal compliance of their security policies and their data disclosure procedures, issuing mainly privacy enhancement recommendations. The authority also examined 58 complaints regarding cases of privacy violations in the electronic communications sector.

The Civil and Penal Courts are also competent to hear cases of violation of the relevant data protection legislation. Civil liability is possible on the basis of Article 57 of the Civil Code (right to personality) and tort law of Article 914 of the Civil Code. Criminal liability is also possible on the basis of Article 370(b) (breach of confidentiality of phone calls) and 370(c) (illicit copying and disclosure of data to third parties) of the Penal Code.

ii Recent enforcement cases

In what may be the most serious data leak case yet to be reported in Greece, the General Secretariat for Information Systems (GSIS), a department of the Ministry of Finance, was fined €150,000 for its failure to implement adequate security measures to protect its databases, which lead to the leak of personal data concerning the vast majority of Greek taxpayers (Decision 98/2013). A man, aged 35, was arrested and brought before a prosecutor for unlawful possession of personal data of 9 million people (more than 80 per cent of Greece's population). The personal data illegally extracted from the GSIS database included names of individuals as well as their tax numbers, home address and vehicle licence plate numbers.

In another data leakage case, the DPA found a major music label, a private company, in breach of Article 10 of the DPL (regarding security measures) and imposed a €10,000 fine for failure to have appropriate organisational and technical measures in place to prevent such a data leak. According to the relevant DPA decision (Decision 59/2012), the website of the company had been hacked and personal data (including names, e-mail addresses and passwords) of 8,385 subscribers and clients were leaked. The Decision also refers to a list of minimum security requirements that must be adopted by data controllers that administer websites. Such requirements include safe coding techniques, data encryption (hashing), limited user account permissions, privacy policy, proactive monitoring and review of security logs, proactive monitoring of data processor's processing, authenticated FTP and controlled remote access tools.

The DPA has also imposed a fine on the administrator of a newspaper website for the publishing sensitive personal data relating to a criminal prosecution. In its Decision 165/2012 the DPA noted that such web publishing can disproportionately affect the rights of individuals, because it can lead to free, universal and uncontrolled access to such information via search engines without any time limitation. The DPA imposed a fine of €10,000 and the newspaper was also ordered to anonymise the information in question. In this context, the DPA also highlighted the data subject's right to object to information published on websites.

Recent DPA decisions for breaches of the regulation on spam include Decisions 99/2013 and 25/2013 imposing a €5,000 fine and a €15,000 fine respectively on entities for illegal collection of personal data and use for direct marketing in breach of the spam regulation (Article 11 Law 3471/2006). In the latter case, the authority considered the great number (433,695) of e-mail addresses used and the fact that the company was reluctant to cooperate with the authority during an audit.

iii Private litigation

Damage claims by data subjects are possible under the DPL although the actual existence of damage will often be difficult to prove. The competent court can also award compensation for moral damages suffered by a data subject, which is set by law at a minimum of €5,870 (unless a smaller amount was requested or the breach was caused by negligence). A claim can also be based on Article 57 of the Civil Code (the right to personality) and the tort law of Article 914 of the Civil Code.

Ins a very recent case (Athens Court of Appeals, 3,808/2014), the publication of photos of private moments in a newspaper is not informative to the public and it only serves the demand and profitability of the newspaper in violation of the principle of proportionality. The amount of €50,000 was awarded by the court for (non-pecuniary) moral damages suffered by the plaintiff.

Further, according to Decision 1,437/2014 of the Athens Court of Appeal, a bank hired a debt collection agency to recover a debt from one of its private clients. For this purpose the bank disclosed the client's personal information to the agency without having previously informed him. The client was surprised to receive the agency's calls on his personal cell phone and also at his wife's shop, which caused him great frustration. The amount of €6,000 was awarded by the court for moral damage suffered by the client.

Criminal courts have been examining data protection cases. In a recent case examined by the Supreme Court (1,110/2013), the defendant had illegally collected sensitive personal data about a judge, which he further used as evidence to support his claims against the judge in a civil litigation procedure. The court found the defendant guilty of a violation of privacy.

According to Decision 499/2013 of the Supreme Court, a journalist collected sensitive personal data regarding the sex life of a priest, which he further broadcast on the TV on the pretext of a journalistic research into corruption. The Court found the defendant guilty and ruled that the above actions exceeded the intended informational purposes in violation of the principle of proportionality.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The DPL will apply when data processing is carried out by a data controller or data processor with a seat in Greece, or by a data controller with no seat in the EU/EEA, which for the purposes of processing personal data, makes use of equipment, automated or otherwise, located in Greece, unless such equipment is used only for transit purposes. Therefore, when the data controller's seat is outside the EU/EEA (and the data controller does not use any data processor with a seat in Greece), the DPL will not apply if equipment (e.g., servers) located in Greece is used only for transit purposes. The PDA

has issued no further official guidance on this matter and the authority often refers to the Article 29 Working Party Opinion 8/2010 on this issue, according to which 'as [the transit element] is an exception to the equipment criterion, it should be subject to a narrow interpretation', especially in cases of services merging pure transit and added value services, including spam filtering or other manipulation of data at the occasion of their transmission (e.g., the service runs java scripts or installs cookies with the purpose of storing and retrieving personal data).

Moreover, pursuant to the DPL, a data controller with no seat in the EU/EEA but who, for the purposes of processing personal data, makes use of equipment, automated or otherwise, located in Greece, must appoint a local representative based in Greece. Such appointment must be notified to the DPA.

IX CYBERSECURITY AND DATA BREACHES

The general principles on data safety are included in the DPL, which uses generic language so as to ensure broad applicability and enforceability. A data controller must implement 'appropriate organisational and technical measures' to secure data and protect them against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access as well as any other form of unlawful processing. Such measures must 'ensure a level of security appropriate to the risks presented by processing and the nature of the data in question'.

Moreover, the DPA can issue guidelines, regulations and directives to further regulate the level of security, the computer and information infrastructure and any specific security measures required for each category and processing of data, and to suggest the use of privacy-enhancing technologies. Relevant is the DPA Directive 1/2005 with regard to data deletion requirements and procedures and the DPA Guidelines on Security Policy, Security Plan and Disaster Recovery and Contingency Plan.

The use of data security technology (e.g., monitoring software) in the workplace is particularly relevant in this context. Such monitoring is permitted under specific circumstances. The DPL makes no specific reference to the use of such monitoring tools, but basic principles and guidelines on the use of monitoring tools in the workplace are included in the Privacy at Work Directive. The Directive provides that apart from the general data collection and processing provisions included in the DPL, the following principles apply to the use of monitoring technologies in the workplace:

a necessity: the form and monitoring of technology must be absolutely necessary for a specific purpose;

b finality: personal data must be collected only for a specified and legitimate purpose and be stored separately;

c transparency: the employees must be properly informed about the monitoring systems in place;

d legitimacy: the data collection and processing purpose must be legitimate; and

e proportionality: no other adequate and less intrusive measure should be available.

With regard to the providers of public communication networks or public electronic communication services in particular, ADAE Decision 205/2013 and the DPA and

ADAE Joint Act 1/2013 are applicable. The ADAE Decision 205/2013 (Regulation for the Safety and Integrity of Networks and Electronic Communications Services) defines the technical and organisational measures that need to be implemented by public communications providers to ensure data security, including reference to business impact analysis, business continuity, penetration tests, vulnerability assessments, physical security, backups, power management, logical access controls, security zones, firewalls, VPNs, intrusion detection systems, event logging, security incident management. Further, the Joint Act also includes data safety guidelines in the context of the data retention obligations imposed by Law 3,917/2011 (implementing Directive 2006/24/EC) on public communications providers and refers to the technical and organisational measures that need to be implemented to ensure data security. The measures include the appointment of a data security officer, encryption, data separation, business continuity, physical security, backups, logical access controls, security zones, event logging, security incident management, data destruction policy and internal controls.

We note that other sector-specific regulations (e.g., banking data, public sector data, military data) demand advanced security measures to be in place. For instance, military regulation makes reference to the levels of classified information, the criteria to be met for persons who have access to such information and to the implementation of measures that ensure secure storing and transferring of such information. In particular, classified information must not be stored on hard disks but on floppy disks and special physical security measures must be implemented. Copies of classified documents can be made only under specific circumstances and with the use of designated computers and copy machines, with restricted access. Highly classified documents are stored in secure physical locations and access to such documents is permitted only to specific individuals and exclusively within such locations.

With regard to data-breach reporting, Article 37 of Law 4,070/2012 sets out that providers of public communication networks or public electronic communication services must report any security breach 'which had a significant impact on the operation of the networks or the service' to the regulator, the National Telecommunications and Post Commission. Moreover, a notification obligation in case of personal data breaches is imposed on all providers of publicly available electronic communications services (ISPs and other telecoms providers), which must notify both the ADAE (no later than 24 hours after the detection of the personal data breach) and customers about such breaches. The ADAE recently published an online notification form for personal data breaches (in compliance with EU Regulation No. 611/2013 on the notification of personal data breaches).[3]

Finally, private and public actors who need to develop network and information security policies and enhance their capability to prevent, detect and respond to network and information security incidents can consult the guidance provided by the European Network and Information Security Agency. The Agency, an EU body of experts based in Heraklion, Greece, also collects and analyses data on security incidents in Europe and

3 www.adae.gr/en/citizen-services/notification-of-personal-data-breaches/.

promotes risk assessment and risk management methods to enhance the capability to deal with information security threats.

X OUTLOOK

An issue gradually gaining the attention of the DPA is the use of smart devices by employees (bring your own device or 'BYOD'). The DPA is expected within the next year to publish either guidelines or a directive on BYOD, which will address data privacy and safety considerations and suggest appropriate technical and organisational data safety measures.

The implementation of internet of things technologies is another issue of importance in Greece. As the use of wireless machine-to-machine technology has already been reviewed by the DPA within the context of e-Call, an EU initiative aimed at bringing rapid assistance to motorists involved in a collision, the DPA has already included the internet of things onto its agenda.

Finally, Greece has signed the Council of Europe's Convention on Cybercrime but, at the time of writing, has not yet ratified it.[4] A committee has been established to discuss the draft for the ratification of the Convention, which is expected to be concluded by the end of 2014. The same committee will also work on the implementation of Directive 2013/40/EU on attacks against information systems.

4 http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

Appendix 1

ABOUT THE AUTHORS

GEORGE BALLAS

Ballas, Pelecanos & Associates LPC

George is senior and managing partner at Ballas, Pelecanos & Associates LPC and heads the firm's prominent IP, IT & CT practice group.

He read law at the Universities of Athens and Paris and was admitted to practise in Athens in 1972.

His diverse career includes holding the posts of Secretary General, Hellenic Parliament; board member, Public Power Corporation; chairman, PPC Insurance Board; chairman, Association for the Establishment of Libraries; general legal counsel and member of the board, Fiat Auto Hellas SA; lead outside counsel for Greece, Microsoft Corporation and Microsoft Hellas SA.

He is a member of the Athens Bar Association, the International Bar Association and the International Trademark Association, an advocate before the Supreme Courts of Greece and a qualified European patent attorney.

In addition to heading the firm's litigation practice in complex pharmaceutical patents and anti-counterfeiting cases, he regularly advises clients in developing and managing strategic initiatives for optimising intellectual asset protection, exploitation and enforcement. He also advises Fortune500 companies on contentious and non-contentious aspects of media, technology and telecommunications law. He has authored articles and contributed chapters to a variety of IP, IT & CT publications and has lectured on patent issues.

George speaks Greek, English, French and Italian.

THEODORE KONSTANTAKOPOULOS

Ballas, Pelecanos & Associates LPC

Theodore Konstantakopoulos is an associate and member of the firm's IP, IT & CT group, the company, tax and employment group and the consumer rights group.

Theodore has been a member of the Athens Bar Association since 2005 and is entitled to argue cases before the lower courts.

A graduate of the Athens University Law School (LLB), Theodore earned a master of laws degree (MLE, *summa cum laude*) from Leibniz University, Hanover, Germany in European company law and e-commerce/consumer protection law, following which he was awarded a second master of laws degree (LLM) from Queen Mary College, University of London in computer and communications law. Theodore is a PhD candidate at the Athens University Law School, working on his thesis on search engines and IP law-related issues.

Theodore's practice is focused on contentious trademark matters, particularly on copyright, trademark infringement and unfair competition litigation. He advises and litigates on all aspects of electronic communications and information technology law, in particular electronic communications and telecoms law, and data protection. Theodore also advises on company law and product liability matters.

Theodore has contributed commentaries on intellectual property issues such as the extension of the duration of copyright and its policy implications. Theodore speaks Greek, English and German.

BALLAS, PELECANOS & ASSOCIATES LPC
10 Solonos Street, Kolonaki
106 73 Athens
Greece
Tel: +30 210 36 25 943
Fax: +30 210 36 47 925
george.ballas@balpel.gr
theodore.konstantakopoulos@balpel.gr
www.ballas-pelecanos.com