ICLG

The International Comparative Legal Guide to:

Data Protection 2017

4th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bae, Kim & Lee LLC
Bagus Enrico & Partners
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Cuatrecasas
Dittmar & Indrenius
Drew & Napier LLC
Ecija Abogados
ErsoyBilgehan
Eversheds Sutherland
GANADO Advocates
Gilbert + Tobin
GRATA International
Hacohen & Co.
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
LPS L@w
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at Law Ltd.
Portolano Cavallo
Rato, Ling, Lei & Cortés Lawyers
Rossi Asociados
Subramaniam & Associates (SNA)
Wikborg Rein Advokatfirma AS

global legal group

global legal group

Contributing Editors
Anita Bapat and Aaron P. Simpson, Hunton & Williams

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Paul Mochalski

Sub Editor
Hollie Parker

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
May 2017

ISBN 978-1-911367-50-5
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Cyprus

Anastasios Kareklas

Koushos Korfiotis Papacharalambous LLC

Georgia Charalambous

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Processing of Personal Data (Protection of the Individual) Law 138(I)/2001 as amended to date ("**The Law**").

1.2 Is there any other general legislation that impacts data protection?

Other general legislation includes:

- The Law N.28(III)/2001 implementing the Convention for the Protection of Individuals with regard to automatic processing of Personal Data and the Law N.30(III)/2003 implementing the Additional Protocol to the said Convention; and
- The Regulation of Electronic Communications and Postal Services Law of 2004, N.112(I)/ 2004 as amended to date.

1.3 Is there any sector-specific legislation that impacts data protection?

The Prevention and Suppression of Money Laundering Activities Law (N.188(I)/2007), for example, imposes on the Compliance Officers of credit institutions the obligation to prepare and update lists categorising low and high-risk clients with reference to their names, account numbers, etc.

1.4 What is the relevant data protection regulatory authority(ies)?

The Office of the Commissioner for Personal Data Protection ("**The Commissioner**").

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"

  "Personal data" or "data" means any information relating to a living data subject; consolidated data of a statistical nature, from which the data subject cannot be identified, are not deemed to be personal data.

- "**Sensitive Personal Data**"

  "Sensitive data" means data concerning racial or ethnic origin, political convictions, religious or philosophical beliefs, participation in a body, association and trade union, health, sex life and sexual orientation, as well as data relevant to criminal prosecutions or convictions.

- "**Processing**"

  "Processing" or "processing of personal data" means any operation or set of operations which is performed by any person upon personal data, whether or not by automatic means, and includes the collection, recording, organisation, preservation, storage, alteration, extraction, use, transmission, dissemination or any other form of disposal, connection or combination, blocking, erasure or destruction.

- "**Data Controller**"

  "Controller" means any person who determines the purpose and means of the processing of personal data.

- "**Data Processor**"

  "Processor" means any person who processes personal data on behalf of the controller.

- "**Data Subject**"

  "Data subject" means the natural person to whom the data relate and whose identity is known or may be ascertained, directly or indirectly, in particular the reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, political or social identity.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  This is not applicable.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  See "Access to Data" in section 4 below.

- **Lawful basis for processing**

  Personal data shall be processed fairly and lawfully. The processing of personal data is lawful when the data subject consents, except where processing is necessary:

  - for compliance with a legal obligation in which the controller is subject pursuant to laws or regulations of the Republic of Cyprus or the European Union;

- for the performance of a contract to which the data subject is party, or in order to take measures at the data subject's request prior to entering into a contract;
- in order to protect the vital interests of the data subject;
- for the performance of a task carried out in the public interest or in the exercise of the public authority vested in the controller or a third party to whom the data are communicated; and
- for the purposes of the legitimate interests pursued by the controller or by the third party to whom the personal data are communicated, on the condition that such interests override the rights, interests and fundamental freedoms of the data subjects.

- **Purpose limitation**

  Personal data should be collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes. It is understood, however, that the subsequent data processing for:
  - historical, statistical or scientific purposes;
  - the purposes of the Director of the Inland Revenue Department of the Ministry of Finane; and
  - the promotion of safety or defence of the Republic of Cyprus or public security or investigation, determination and prosecution of criminal offences,

  is not inconsistent with the purposes for which the data were collected.

- **Data minimisation**

  See Proportionality and Retention below.

- **Proportionality**

  Personal data shall only be processed to the extent they are relevant, appropriate and not excessive in relation to the purposes of processing. The principle of proportionality is not applicable for personal data processed for the purposes of:
  - the Director of the Inland Revenue Department of the Ministry of Finance; and
  - the promotion of safety, or defence of the Republic of Cyprus or the public security or investigation, determination and prosecution of criminal offences.

- **Retention**

  Personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary, in the Commissioner's discretion, for the fulfilment of the purposes for which they were collected and processed. After the expiry of this period, the Commissioner may, by a reasoned decision, allow the preservation of personal data for historical, scientific or statistical purposes if he considers that the rights of the data subjects or third parties are not affected.

- *Other key principles – please specify*

  Personal data shall be accurate, and where necessary, updated. See section 4 below for further detail.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  Every person has the right to know whether the personal data relating to him are or were processed. To this end, the controller must reply to him in writing. The data subject has the right to ask for and receive from the controller without excessive delay and expense information about, *inter alia*, their data which have undergone processing and the purpose of processing.

- **Correction and deletion**

  The data subject has the right to request and obtain from the controller, without undue delay and expense: the rectification, erasure or blocking of data; and the notification of any rectification, erasure or blocking to third parties to whom the data have been notified unless this is impossible or involves a disproportionate effort.

- **Objection to processing**

  The data subject has the right to object, at any time, on compelling legitimate grounds relating to his particular situation, to the processing of data relating to him. The objection shall be in writing and addressed to the controller, and must contain a request for specific action to be taken, such as rectification, temporary abstention from use, blocking, abstention from transmission or erasure.

- **Objection to marketing**

  See section 7 below.

- **Complaint to relevant data protection authority(ies)**

  It is within the Commissioner's responsibilities to examine complaints by any person regarding the protection of their rights when they are affected by the processing of their data, and applications by third parties on the implementation of this law. The Commissioner decides whether to conduct a review of the complaint or the application or whether to continue or to discontinue the examination of the complaint.

- *Other key rights – please specify*

  This is not applicable.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

The controller must notify the Commissioner in writing about the establishment and operation of a filing system or the commencement of processing except where:

- processing is performed solely for purposes directly connected with work to be done and is necessary for the fulfillment of a legal obligation or for the performance of a contract provided that the data subject has been previously informed of;
- the processing concerns customers or suppliers of the data subject provided that the data are neither transferred nor communicated to third parties; and
- processing is performed by a society, association, company or political parties and concerns data related to their members, provided that these members have given their consent and the data are neither transferred, nor communicated to third parties.

The Courts and the public authorities are not regarded as third parties, provided that the transmission or communication is provided by law or Court decision:

- Processing is performed by doctors or other persons who provide health services and concerns medical data, provided that the controller is bound by medical confidentiality or confidentiality required by law or code of conduct and the data are neither transferred, nor communicated to third parties.

- Processing is performed by advocates and concerns the provision of legal services to their clients, provided that the controller is bound by confidentiality required by law and the data are neither transmitted, nor communicated to third parties, except in cases where it is necessary and is directly connected with a request from their clients.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

The duty arises per data controller, who shall register the personal data per processing purpose or filing system.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

The duty to notify arises for every data controller, irrespective of legal status, whether it is a legal or a natural person, or a public authority. Data controllers established outside the Republic of Cyprus shall appoint a Cypriot representative whose details must be registered with the Commissioner.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

The controller must state: (a) his (or if not established in Cyprus, his representative's) full name, business name or title and his address; (b) the address where the filing system is established or where the main equipment necessary for the processing is installed; (c) a description of the purpose of the processing of the relevant data; (d) a description of the category/ies of data subjects; (e) the categories of data; (f) the period of time for which he intends to carry out the processing or keep the filing system; (g) the recipients or categories of recipients to whom he communicates or may communicate the data; (h) the proposed transmissions of data to third countries and the purpose thereof; and (i) the basic characteristics of the system and the measures for the security of the filing system or of the processing.

5.5 What are the sanctions for failure to register/notify where required?

Omission to notify the establishment and operation of a filing system or the commencement of processing is a criminal offence; see question 13.4 below with regards to the penalties that may be imposed. In addition, the Commissioner may impose the following administrative sanctions in case of contravention with the obligations arising from the Law and from every other regulation concerning the protection of individuals with regard to the processing of personal data: (a) a warning with a specific time-limit for termination of the contravention; (b) a fine of up to €30,000; (c) temporary revocation of a licence; (d) permanent revocation of a licence; or (e) the destruction of a filing system or the cessation of processing and the destruction of the relevant data.

5.6 What is the fee per registration (if applicable)?

This is not applicable.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

Any material change of the information referred to in question 5.4 must be notified in writing and without delay by the controller to the Commissioner.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

- Processing of sensitive personal data is prohibited unless, *inter alia*, such processing is necessary in order for the controller to fulfil its obligations or carry out its duties in the field of employment law and provided that the Commissioner's prior approval has been obtained.
- If the controller intends to combine filing systems, at least one of which contains sensitive data or if such combination results in the disclosure of sensitive data, or if for the combination to be carried out a single code number is to be used, the combination is permitted only with the prior approval of the Commissioner.
- Transmission of data, which have undergone processing or are intended for processing after their transmission, to any country shall be permitted after a licence from the Commissioner. For further details on this, consult section 8 below.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

Prior approval is obtained by filing the relevant application form to the Commissioner's office. The Commissioner responds, accordingly, as soon as practically possible. More specifically, the approval for combination of filing systems is obtained after a hearing of the data controller before the Commissioner and the payment of the fees determined by the relevant Regulations.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

This is optional.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

Even if organisations, companies or public authorities are not currently required to appoint a Data Protection Officer, with the new EU Regulation (GDPR) coming into force in 2018, it should be regarded as extremely beneficial to do so. This is mainly because of the high costs of non-compliance with the GDPR. In addition, an organisation in Cyprus which plans to proactively appoint a DPO will be in a much better position than others which do not, both when dealing with supervisory authorities, business partners or individuals with regard to privacy and data protection issues. Nevertheless, all organisations whose core activities involve large-scale processing of personal and, in particular, special categories of

data, will be required by law to appoint a DPO under the GDPR. It is thus advisable to create a GDPR-compliant environment within the organisation prior to the enforcement of the GDPR in order to be ahead of the various challenges which may arise down the line.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

This is not applicable.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

Marketing communications via post are regulated by Article 15 of the Law, whereas other marketing communications are covered by Article 106 of the Regulation of Electronic Communications and Post Law N.112(I)/2004. As far as post marketing communication is concerned, no marketing communications shall occur unless the data subject provides his written consent, except for data subjects whose data were processed on the enactment date of the amending law N.105(I)/2012 in which case data processing may continue until the data subjects opt-out. With regards to other marketing communications, the prior free and informed consent of the data subject is required, except where the data subject is an existing customer of the data controller and the marketing communications relate to the promotion of goods or services similar to those already received from the data subject by the data controller, in which case direct marketing is allowed provided the data subject is given the opportunity to, free of charge and easily, opt-out. For the consent to be deemed free, it has to be given in addition to any terms and conditions for the provision of goods or services by the data controller to the data subject and, according to article 11 of the Law, it must set out the identity of the data processor, the purpose of the processing and the potential recipients of the data.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

Yes. The Commissioner has, since 2005, dealt with 11 cases of marketing restrictions violations. The fines imposed vary within the range of €400–€8,000 and mitigating and aggravating factors, such as whether the violation was a one-off incident or was repetitive, whether the perpetrator immediately admitted to a breach, whether the number of complainants was small or large, and whether measures to avoid future breach of the law were taken or not and if this influenced the Commissioner's decision on the sanction to be imposed.

7.3 Are companies required to screen against any "do not contact" list or registry?

Such list exists for communications with content of a political nature.

7.4 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

See question 5.5 above.

7.5 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

The law requires explicit opt-in consent for all types of information storing except for the instances stipulated in question 7.6 below.

7.6 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

Consent is implied for any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or where it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

7.7 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

The relevant authorities are the Commissioner for the Protection of Data and the Commissioner of Electronic Communications and Postal Services. There has been no published enforcement actions to date.

7.8 What are the maximum penalties for breaches of applicable cookie restrictions?

See question 5.5 above.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad.

The transfer of personal data to a third country is prohibited unless the country in question ensures an adequate level of protection. An exception to this rule is the transfer of personal data to an EU Member State which is generally acceptable and not subject to a notification to the Commissioner.

However, the transfer of personal data to a country which does not ensure an adequate level of protection is exceptionally allowed, with the Commissioner's authorisation, if one or more of the following conditions are satisfied:

(1) the data subject has consented to the transfer;

(2) the transfer is necessary:

(a) to protect the vital interests of the data subject; or

(b) for the conclusion and performance of a contract between

the data subject and the controller or between the controller and a third party in the interest of the data subject; or

(c) for the implementation of precontractual measures taken at the request of the data subject.

(3) the transfer is necessary for dealing with exceptional necessity to safeguard overriding public interest;

(4) the transfer is necessary for the right to recognition, exercise or defence before the court; and

(5) the transfer is made from a register which according to the law is intended to provide information to the public.

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Where the adequate level of protection of the country in question is not satisfied, there are a number of conditions under which it could be possible to obtain permission to the transfer of personal data.

- One such condition is the presentation of adequate guarantees stemming from appropriate contractual terms (contractual clauses) which are usually included in a written agreement entered into by the sender of the data with the recipient who is established in a third country.

Taking the example of employees' personal data, the EU Commission has approved contractual clauses (standard contractual clauses) which can be used/be sufficient guarantee to justify the authorisation for transfer of the personal data of employees in a country that does not provide adequate protection of personal data.

- As of July 2016, the transmission of data in the US may be allowed if the company which will be transmitted data if certified under the EU-US Privacy Shield, for which the U.S. Department of Commerce is responsible.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

The disclosure, to any country, of data which have been or are intended for processing after transmission, is permitted on the Commissioner's authorisation.

To this end, the Commissioner takes into account in particular:

- the nature of the data;
- the purpose and duration of the processing;
- the relevant general and special rules of law;
- codes of conduct, security measures for the protection of data; and
- the level of protection of the countries of origin, transit and final destination of the data.

See section 5 above for further details on the registration/notification or prior approval procedure.

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

Due to the fact that corporate whistle-blowing is not regulated under Cyprus law, in order for any whistle-blower hotlines to be lawful, they should comply with the general principles set out in sections 3, 4 and 5 above. Regarding whistle-blower hotlines, the Commissioner's Annual Report refers companies to Article 29 Working Party's opinion 1/2006. In principle, in case the whistle-blower hotline is put in place to protect a legitimate interest of the data processor, the latter shall ensure that the legitimate interest is not overridden by the interests for fundamental rights and freedoms of the data subject(s).

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

The Commissioner advises controllers to avoid anonymous reporting or to have internal procedures for handling such reporting.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

See section 5 above.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

According to Article 29 Working Party's opinion 1/2006, the requirement of clear and complete information on the system obliges the controller to inform data subjects about the existence, purpose and functioning of the scheme, the recipients of the reports and the right of access, rectification and erasure for reported persons.

9.5 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

See question 10.4 below.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Yes. The person responsible for the operation of CCTV, under Article 7 of the Law, must submit a written notification to the Commission, for the purpose for which they use the system, providing the required information, unless covered by the exceptions that are provided for by law.

Individuals who are about to be recorded on CCTV must be informed of the recording and must be given the right to "refuse" by refusing to enter the building or public space, in which the CCTV is operating. To this end, in order to comply with their obligation to inform, it is acceptable and satisfactory for controllers/operators to post warning signs at points outside the view of the CCTV. There are also cases where it would not be desirable to warn the public. These are cases where the CCTV recording is for state defence purposes, national needs or for the prevention, detection and prosecution of criminal offences and is allowed following the authorisation by the Commissioner (Article 11 (4) of the Law).

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

The employer shall be able to justify the legality and necessity of control and monitoring, and that there is no other less intrusive method for carrying out the objectives pursued. The legitimate interest invoked by the employer, in order to be justified, must prevail over the rights, interests and fundamental freedoms of employees.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Employers must in all cases inform the employees about the purpose, manner and duration of control and monitoring they intend to apply prior to the beginning of the monitoring. For this purpose, it is good practice for the employer to adopt a written policy for determining the parameters of telephone use, computer, internet, other electronic means of communication and material/equipment of the company/organisation of employees and ways/systems with which the employer will monitor/control its use. Secret surveillance or monitoring of employees is never permitted without the employees having been previously updated.

10.4 To what extent do works councils/trade unions/ employee representatives need to be notified or consulted?

According to the Commissioner's guidelines on the subject, it is good practice for employers to consult employee representatives and trade unions prior to the installment and use of CCTV or other control measures.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Where the use of such systems involves the collection, analysis and storage of personal data relating to employees, the data controller must notify the Commissioner in writing for the establishment and operation of a file or initiating of the processing.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

An application for a transmission licence must be submitted to the Commissioner. It should be accompanied by appropriate Standard Contractual Clauses (approved by the European Commission Decision 2010/87/EC), signed by the data exporting company, (the controller who transfers the personal data) the data importer company (the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer) and the contractor. A necessary prerequisite for obtaining a licence would be the inclusion of the relevant annex of the data importer companies/subcontractors that will provide cloud computing services to the transmitted data (email) of the data exporter company.

The Commissioner points out the company's obligation, as a controller, in compliance with the provisions of Article 11 (1) of the Law, to inform, *inter alia*, the data subjects i.e. people (customers, partners, etc.) of the company which communicate with the company through emails, about the possible transmission of their data and the provision of cloud computing services by the importer company and contractor of the data in the US and subsidiaries of the latter as subcontractors in Europe and third countries, but also on their ability to exercise their right of access and objection.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

These are the obligations imposed on the data importer (processor) as outlined in *Clause 5* of the 2010/87 Decision.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are no relevant legal provision or guidelines.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

According to the Law, the controller must take the appropriate organisational and technical measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing. Such measures shall ensure a level of security which is appropriate to the risks involved in the processing and the nature of the data processed. As far as providers of publicly available electronic communications services ('the provider') are concerned, such technological protection measures should render the data unintelligible to any person who is not authorised to access them.

'Data shall be considered unintelligible' if:

(a) it has been securely encrypted with a standardised algorithm; or

(b) it has been replaced by its hashed value calculated with a standardised cryptographic keyed hash function, so that it cannot be ascertained by available technological means by any person who is not authorised to access the key.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

In the event of a personal data breach, the provider of publicly available electronic communications services shall notify without delay the violation to the Commissioner of Electronic Communications and Postal Services.

The notification to the subscriber or individual affected shall not be required if the provider demonstrates to the satisfaction of

the Commissioner that the appropriate technological protection measures, such as the encryption measures mentioned in question 13.1 above, have been taken and that those measures were applied to the data breach involved.

The notification shall include the following components:

(a) the conditions under which the event occurred and the nature of the violation;

(b) the contact point of the provider;

(c) proposed measures to mitigate the adverse effects of the breach;

(d) the consequences of the breach; and

(e) corrective measures, which the provider is taking to address the breach.

The content of the notification to the competent national authority is outlined in ANNEX I of the Commission Regulation (EU) No 611/2013.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

If the violation may adversely affect the personal data or privacy of a subscriber or an individual, the provider shall notify without delay to the subscriber affected or affected individual, at least the nature of the breach and the contact points where more information can be obtained. He shall also propose measures to mitigate any adverse effects of the breach.

If the provider does not proceed with the notification to the subscriber or the affected person, the Commissioner with the approval of the Commissioner for Personal Data Protection, may request to make the notification.

The notification to the subscriber or individual affected shall not be required if the provider demonstrates to the satisfaction of the Commissioner that the appropriate technological protection measures have been taken and that those measures were applied to the data breach involved.

The content of the notification to the subscriber or individual is outlined in ANNEX II of the Commission Regulation (EU) No 611/2013.

13.4 What are the maximum penalties for security breaches?

If as a result of the breach:

(a) the perpetrator purported to gain to himself/herself or another, unlawful property benefit or harm a third party; or

(b) the free functioning of the Government of the Republic or to national security have been jeopardised,

the guilty party shall be punished with imprisonment up to five years or a fine up to €8,543 or to both such penalties.

If the violation has been committed by negligence, the guilty party shall be punished with imprisonment up to three years or a fine not exceeding €5,125.80 or with both such penalties.

In addition, please consult question 5.5 above regarding the sanctions that could potentially be imposed by the Commissioner.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
To enter, even without informing the interested parties, any office, professional or business premises or vehicle, excluding any residence.	To impose an administrative fine of €5,000 to any person who fails to comply with the Commissioner's instructions or obstructs the Commissioner's investigation.	The Commissioner does not have the jurisdiction to impose criminal sanctions.
To access any records (except where such records are protected by advocates privilege or they concern the identity of partners in archives kept for reasons of national security or the investigation of particularly serious crimes) and collect documents, data and information.	See question 5.5 above.	N/A
To be accompanied by experts during the carrying-out of the investigation.	N/A	N/A
To summon any witness or any person to provide any relevant documents or other evidence.	N/A	N/A
Entitlement to the police's assistance for the execution of its enforcement powers.	N/A	N/A

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

Upon the submission of a complaint, the Commissioner's office contacts the accused person (respondent) requesting its comments/position/opinions on the incident of the complaint. If the Commissioner finds that there is a *prima facie* violation of the data protection legislation, it invites the respondent to provide its further comments/position/opinions and argue against the imposition of a sanction. At this point, the Commissioner issues her reasoned decision. This process was, for example, followed in the investigation of a complaint against a hospital for the loss of a patient file, where the Commissioner, after investigating the complaint, imposed a fine of €2,000.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Data exporters must inform the Commissioner of any third country legislation that the data importer is subject to, providing for the statutory disclosure of the transferred data to public authorities of that country.

15.2 What guidance has the data protection authority(ies) issued?

The Commissioner advises data exporters to scrutinise such legislations against the Art.29 Working Party Working document titled "Essential Guarantees".

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

There is no relevant case law issued in the past 12 months.

16.2 What "hot topics" are currently a focus for the data protection regulator?

The application and effect of the forthcoming EU General Data Protection Regulation (GPDR) in 2018 and its various uncertain developments resulting from its automatic transposition into Cyprus Law has been one of the main issues of focus of the Commissioner's office. These developments can be briefly outlined as follows:

(a) Contrary to what is mentioned in section 6 above, it will be mandatory for Cypriot public authorities or companies whose activities are predominantly based and dependent on large-scale personal data processing to appoint a data protection officer. It is anticipated that this development will put unprecedented pressure on all organisations with such involvement since their non-compliance with the new associated rules will prove very costly.

(b) The GDPR will be the first law to explicitly cover the right to erasure (also known as the 'right to be forgotten'). Unlike the current Directive, the onus to justify the processing will now lie on the controller.

(c) The issue of 'retention' of data is likely to draw attention in the upcoming years with regard to the revised 'storage limitation' and 'data minimisation' principles as construed within the GDPR.

The use of drones is also an issue which requires special attention and the Commissioner's office suggests, as a potential solution, the introduction of specialised European or domestic legislation.

Anastasios Kareklas
Koushos Korfiotis Papacharalambous LLC
20 Costis Palamas str., Aspelia Court
1096 Nicosia
Cyprus

Tel: *+357 22 664 555*
Email: *akareklas@kkplaw.com*
URL: *www.kkplaw.com*

Anastasios graduated from the University of Sussex Law School (LL.B.) in 2015. In 2016, he obtained an LL.M. in Computer and Communications Law at Queen Mary, University of London. Anastasios currently works as a Trainee Lawyer at Koushos Korfiotis Papacharalambous LLC. He is specialised in E-Commerce Law, Data Protection Law and Information Technology Law.

Georgia Charalambous
Koushos Korfiotis Papacharalambous LLC
20 Costis Palamas str., Aspelia Court
1096 Nicosia
Cyprus

Tel: *+357 22 664 555*
Email: *gcharalambous@kkplaw.com*
URL: *www.kkplaw.com*

Georgia obtained her LL.B. at the University of Southampton in 2013. In 2014, she completed the Legal Practice Course at BPP Law School in London and also obtained the European Master in Law and Economics. She joined Koushos Korfiotis Papacharalambous LLC as a lawyer in 2017 after successfully undertaking the Cyprus Legal Council exams.

KOUSHOS KORFIOTIS PAPACHARALAMBOUS LLC

ADVOCATES & LEGAL CONSULTANTS

Koushos Korfiotis Papacharalambous LLC comprises more than 20 lawyers based in our offices in Nicosia. KKP is a full-service law firm with an industry focus on financial services including financial, insurance and banking institutions, intellectual property, real estate and construction, corporate and securities law. The firm operates in multi-disciplinary teams, which allow us to provide clients with individualised and expert advice. Our team of lawyers has more than 30 years of experience, combining an extensive knowledge of the Cypriot legal system with an in-depth understanding of international and European law. Partners of the firm are members of professional legal organisations such as the International Trademark Association (INTA), the European Communities Trade Mark Association (ECTA), MARQUES, the Pharmaceutical Trade Marks Group (PTMG), the International Tax Planning Association, and the Chartered Institute of Arbitrators, while a number of them are also endorsed and highly rated by the world's leading international legal directories, including *The Legal 500*.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com