ICLG

The International Comparative Legal Guide to:

Data Protection 2018

5th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Anderson Mōri & Tomotsune
Ashurst Hong Kong
BSA Ahmad Bin Hezeem & Associates LLP
Clyde & Co
Cuatrecasas
DQ Advocates Limited
Ecija Abogados
Fırat İzgi Attorney Partnership
GANADO Advocates
GÖRG Partnerschaft von Rechtsanwälten mbB
Herbst Kinsky Rechtsanwälte GmbH
Holding Redlich
Jackson, Etti & Edu
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
KPMG Law Firm
Lee & Ko
Loyens & Loeff Luxembourg S.à r.l.
Loyens & Loeff N.V.
LPS L@w
Lydian
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
OLIVARES
OrionW LLC
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at law
Pillsbury Winthrop Shaw Pittman LLP
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Subramaniam & Associates (SNA)
Trevisan & Cuonzo Avvocati
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg
global legal group

global legal group

Contributing Editors
Tim Hickman & Dr. Detlev Gabel, White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Executive 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
June 2018

ISBN 978-1-912509-15-7
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapters:

Country Question and Answer Chapters:

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

Cyprus

Loizos Papacharalambous

Koushos Korfiotis Papacharalambous LLC

Anastasios Kareklas

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repeals Directive 95/46/EC (the "**Data Protection Directive**") and leads to increased (though not total) harmonisation of data protection law across the EU Member States.

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

- 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 authority(ies) are responsible for data protection?

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**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**" means an individual who is the subject of the relevant personal data.
- "**Special Categories of Personal Data**" are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.
- "**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents

in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

4 Key Principles

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

- **Transparency**

  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**

  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**

  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.

- **Data minimisation**

  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Accuracy**

  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**

  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Data security**

  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**

  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

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

- **Right of access to data/copies of data**

  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to be determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

  Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**

  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**

  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**

  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights

and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**

  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**

  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**

  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**

  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**

  Data subjects have the right to lodge complaints concerning the processing of their personal data with the data protection authority in Cyprus, if the data subjects lives in Cyprus or the alleged infringement occurred in Cyprus.

- **Right to basic information**

  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Only notification in special circumstances: see question 11.3.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

See question 11.3.

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

See question 11.3.

6.4 Who must register with/notify the data protection authority (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)?

Only notifications in special circumstances: see question 11.3.

6.5 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)?

Only notifications in special circumstances: see question 11.3.

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

Not known yet. Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. Please refer to the online version of the chapter for the updated answer.

6.7 What is the fee per registration/notification (if applicable)?

This is not applicable.

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

This is not applicable.

6.9 Is any prior approval required from the data protection regulator?

This is not applicable.

6.10 Can the registration/notification be completed online?

This is not applicable.

6.11 Is there a publicly available list of completed registrations/notifications?

This is not applicable.

6.12 How long does a typical registration/notification process take?

This is not applicable.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or

processors is only mandatory in some circumstances including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

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

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

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

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on data protection impact assessments and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

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

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party (the "**WP29**") recommends that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the Data Protection Officer; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing. (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?)

Marketing communications are covered by Article 106 of the Regulation of Electronic Communications and Post Law N.112(I)/2004. 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.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

See question 9.1.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

This is not applicable.

9.4 Is/are 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 by 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.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

This issue has been dealt with by the Commissioner who has issued fines against unlawful data processing for marketing purposes by various candidates during political elections. The Commissioner has issued the following guidance:

"Several candidates are targeting paid advertising agencies to send messages on their behalf. In these cases, candidates should themselves provide a list of the recipients' numbers or addresses. If advertisers maintain their own list, they must be able to ensure that they have received the consent of the recipients with regard to the particular type of advertising requested by the candidate (e.g. the recipients have stated that they are interested in receiving political messages from anyone). Candidates should be able to check the list of recipients and the process of sending the messages (consent, deletion file, etc.). In messages sent, it should be clear who the advertiser is who has sent the messages on behalf of the candidate. The above details must be provided in a contract between the candidate and the advertising company, which has the status of data processor."

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

Under the Cyprus Data Protection Law, which will be replaced by the GDPR, 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.

It remains to be seen how these fines will be dealt with post-May 2018.

Please note that this answer was written before changes to Cypriot legislation with regards to the implementation of the GDPR were published. Please refer to the online version of the chapter for the updated answer.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The Regulation of Electronic Communications and Post Law N.112(I)/2004 as amended implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real indication of the individual's wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

This is not applicable.

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

No, there has been no enforcement action.

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

See question 9.6.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the "**EEA**") can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission) or the business has implemented one of the required safeguards as specified by the GDPR.

11.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules ("**BCRs**").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirement when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

* When the controller or the processor intends to transfer special categories of personal data to a third country or to an international organisation on the basis of the appropriate safeguards provided for in Article 46 or on the basis of the binding corporate rules provided for in Article 47, the controller or the processor must inform the Commissioner of their intention before transferring such data.

Without prejudice to the provisions of Articles 46 and 47 of the GDPR, the Commissioner may, on serious public interest grounds, impose on the controller or the processor explicit limitations on the transfer of the specific categories of personal data.

The transmission of specific categories of personal data to a third country or to an international organisation to be carried out by a controller or processor under the derogations for specific situations provided for in Article 49 of the GDPR, requires a data protection impact assessment ("**DPIA**") and prior consultation with the Commissioner.

* Please note that this answer was written before changes to Cypriot legislation with regards to the implementation of the GDPR were published. Please refer to the online version of the chapter for the updated answer.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconducts.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. The WP29 recommends that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. As a rule, the WP29 considers that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be

informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

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

13 CCTV

13.1 Does the use of CCTV require separate registration/ notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

A DPIA must be undertaken with assistance from the Data Protection Officer when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

13.2 Are there limits on the purposes for which CCTV data may be used?

This is not applicable.

14 Employee Monitoring

14.1 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.

14.2 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.

According to the GDPR requirements, other EU Guidance and Directives from the Commissioner, the consent as a legal basis for processing employees' personal data, which should be avoided, were possible due to the imbalance of power between the employer and the employees, which might render the consent in question as not freely given or unambiguous.

14.3 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 installation and use of control measures within the workplace.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident and a process for regularly testing and evaluating the technical and organisation measures for ensuring the security of processing.

15.2 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) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? 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) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of €20 million or 4% of worldwide turnover.

16 Enforcement and Sanctions

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

Investigatory Powers * * Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. Please refer to the online version of the chapter for the updated answer.	**Civil/Administrative Sanction *** * Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. Please refer to the online version of the chapter for the updated answer.	**Criminal Sanction *** * Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. Please refer to the online version of the chapter for the updated answer.
Investigative Powers	The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and access to the premises of the data including any data processing equipment.	N/A
Corrective Powers	The data protection authority has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below).	N/A
Authorisation and Advisory Powers	The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.	N/A

Investigatory Powers *	Civil/Administrative Sanction *	Criminal Sanction *
* Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. Please refer to the online version of the chapter for the updated answer.	* Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. Please refer to the online version of the chapter for the updated answer.	* Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. Please refer to the online version of the chapter for the updated answer.
Imposition of Administrative Fines for infringements of Specified GDPR Provisions	The GDPR provides for administrative fines which can be €20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year.	N/A
Non-Compliance With a Data Protection Authority	The GDPR provides for administrative fines which will be €20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year, whichever is higher.	N/A

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority to impose a temporary or definitive limitation including a ban on processing.

Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. Please refer to the online version of the chapter for the updated answer.

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

This information is not available yet.

Please note that this answer was written before changes to Cypriot legislation with regards to the implementation of the GDPR were published. Please refer to the online version of the chapter for the updated answer.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

This is not applicable.

Please note that this answer may be subject to change by the Cypriot legislation with regards to the implementation of the GDPR which was not published at the time of writing this chapter. Please refer to the online version of the chapter for the updated answer.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do companies typically 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.

17.2 What guidance has/have the data protection authority(ies) issued?

The Commissioner advises data exporters to scrutinise such legislations against the WP29 Working Document titled "Essential Guarantees".

18 Trends and Developments

18.1 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.

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

The office of the Commissioner has been focusing on the prevention of false practices in breach of the Data Protection Laws by both the public and private sector, and in so doing, has issued guidance about a) the DPIAs, b) Records of Processing Activities (Article 30 of the GDPR), c) Certification Bodies, and d) Retention Policies by Authorised Credit Institutions. The Commissioner has also advised for vigilance with cybersecurity threats and also with how third parties may unlawfully process consumers' and users' data.

Loizos Papacharalambous
Koushos Korfiotis Papacharalambous LLC
20 Costis Palamas str.
Aspelia Court
1096 Nicosia
Cyprus

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

Loizos has been a member of the Cyprus Bar Association since 2004. He graduated from the University of Bristol before going on to successfully complete the Bar Vocational Course, becoming a member of Gray's Inn. In 2006, Loizos successfully completed the International and Comparative Commercial Arbitration Diploma with Queen Mary College of the University of London. In 2011, Loizos was admitted as a Member of The Chartered Institute of Arbitrators. Loizos is currently attending courses to obtain a M.Sc. in Finance and Banking. His main areas of practice are commercial and corporate litigation and representation of banks, investment and insurance companies.

Loizos has been the Vice-Chairman of the Cyprus Telecommunications Authority (CYTA), the Vice-President of the Nicosia Bar Association and the Chairman of the Housing Finance Corporation.

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 is a lawyer at Koushos Korfiotis Papacharalambous LLC, with wide-ranging knowledge and experience on IT legal matters both on academic and business levels, with a particular focus on e-Commerce Law and Data Protection Law. Anastasios holds an LL.B (Hons) from the University of Sussex and an LL.M in Computer and Communications Law from Queen Mary University of London (QMUL). Anastasios acts as Data Protection Advisor and is a key member of the Data Protection Team at KKP LLC. He provides consultation on compliance issues and legal advice on data protection for clients.

KOUSHOS KORFIOTIS PAPACHARALAMBOUS LLC

ADVOCATES & LEGAL CONSULTANTS

Koushos Korfiotis Papacharalambous LLC comprises more than 20 lawyers based in our offices in Nicosia. KKP LLC 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 allows 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
- Anti-Money Laundering
- 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
- Cybersecurity
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State 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 Investment Funds
- 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