International
Comparative
Legal Guides

Practical cross-border insights into data protection law

Data Protection 2023

10th Edition

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

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

Cyprus


Michael Kyriakides


Eleni Neoptolemou


Munevver Kasif

Harris Kyriakides

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The Law of 2018 on the Protection of Natural Persons Against the Processing of Personal Data and the Free Movement of Such Data (125(I)/2018) (the **Law**), which was enacted on July 31, 2018, is the main legislation of data protection law in Cyprus. The Law transposed the Regulation (EE) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and replacing Directive 95/46/EC (**GDPR**).

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

Within the jurisdiction of Cyprus there is no other general legislation that impacts data protection, other than the Law on Electronic Communications and Postal Services Regulation of 2004 (112(I)/2004) as amended. However, the European Data Protection Board (**EDPB**) issues general guidance to promote a common understanding of European data protection laws, both across the European Union and around the world. Although the guidelines provided by the EDPB are not considered as legislation, they are considered.

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

Yes, certain pieces of legislation in Cyprus contain certain sector-specific data protection requirements. For example, Law on the Prevention and Suppression of Money Laundering (No. 188(I)/2007) provides that the obliged entities shall retain the relevant personal data for a period of five years after the end of their business relationship with the customer or after the date of the occasional transaction.

1.4 What authority(ies) are responsible for data protection?

The Commissioner for Personal Data Protection is appointed as the supervisory authority for the purposes of the GDPR and has the responsibility to monitor the application of the provisions of the GDPR and the Law in the Republic of Cyprus and other arrangements concerning the processing of personal data (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 ("data subject"). An identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular by reference to an identifier such as a name, an identity number, location data, an online identifier or one or more factors that characterise the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.
- "**Processing**"
  Means any operation or series of operations carried out with or without the use of automated means, on personal data or sets of personal data, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, information retrieval, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion 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 the natural or legal person, or public authority, or agency or other body that processes personal data on behalf of the controller.

- "**Data Subject**"
  Is used to refer to a person who is the subject of the pertinent personal data.
- "**Sensitive Personal Data**"
  Is any information that may be used to identify a specific individual, such as genetic or biometric information, information about their health or sexual life, or information about their political, religious or philosophical views.
- "**Data Breach**"
  Is a security breach that causes personal data to be accidentally or intentionally lost, altered, disclosed to unauthorised parties, 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 Law states that the provisions shall apply to the Republic of Cyprus in accordance with the provisions of Article 3 of the GDPR. Article 3 of the GDPR states that the GDPR is applicable to businesses established within the EU (as a controller or a processor, regardless of whether the processing takes place in the Union or not) withing the context of that establishment. The GDPR applies to businesses outside the EU if they process personal data of data subjects who are in the Union where in relation to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

4 Key Principles

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

- **Transparency**
  Personal information should be handled in a lawful, fair and clear manner. Those in charge of the data (controllers) are required to provide individuals with essential details about how their personal information is collected and used. This information should be given in a brief, easy-to-understand, and easily accessible format, using straightforward language.
- **Lawful basis for processing**
  The processing of personal information is considered lawful only if it complies with the regulations set forth in EU data protection law and the national law. The GDPR provides a comprehensive list of legal grounds for processing personal data, with the following being the most relevant for businesses: (i) obtaining explicit, informed, and unambiguous consent from the individual; (ii) processing that is necessary for fulfilling a contract or carrying out pre-contractual measures requested by the individual; (iii) compliance with legal obligations imposed by EU or Member State laws; or (iv) processing based on the legitimate interests of the controller, except when the controller's interests are outweighed by the fundamental rights and freedoms of the individuals affected.
  It is important to mention that businesses need more compelling reasons to process sensitive personal information. The processing of sensitive data is only permitted under specific circumstances, with the most relevant conditions for businesses being: (i) obtaining explicit consent from the individuals affected; (ii) processing that is necessary within the scope of employment law; or (iii) processing that is necessary for the purpose of establishing, exercising, or defending legal claims.
- **Purpose limitation**
  Personal information can only be gathered for specific, clear, and lawful purposes, and it must not be processed in a way that is inconsistent with those purposes. If a controller intends to use the collected personal data in a manner that does not align with the original purposes, they must: (i) notify the individual about this new processing; and (ii) have a valid legal basis, as outlined previously, to justify such usage.
- **Data minimisation**
  Personal information should be appropriate, pertinent, and kept to a minimum in relation to the purposes for which it is processed. A business should only process the personal data that is genuinely required to fulfil its processing objectives.
- **Proportionality**
  The collection and processing of personal data should be proportionate to the intended purpose. This means that the extent of data collected and processed should not be excessive or disproportionate to what is necessary to achieve the stated purpose. Data controllers should carefully assess and determine the minimum amount of personal data required to fulfil the intended purpose, avoiding unnecessary or intrusive processing.
- **Retention**
  This is the practice of determining and implementing appropriate timeframes for retaining personal data in a secure and controlled manner. It involves establishing policies and procedures to govern the storage and deletion of personal data based on legal requirements, business needs, and the purpose for which the data was collected.
  The GDPR emphasises the principles of purpose limitation and storage limitation, stating that personal data should only be retained for as long as necessary to fulfil its intended purpose. Organisations must have a lawful basis for retention, establish specific retention periods, and practice data minimisation by retaining only necessary and relevant data. They must ensure the security and protection of retained data, and be accountable by documenting retention practices. If personal data is transferred outside the EU, appropriate safeguards must be implemented. Compliance with GDPR principles ensures the protection of individuals' rights and privacy throughout the data retention process.

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**
  An individual has the right to request the following information from a data controller regarding their personal data: (i) confirmation of whether and where the controller is processing their personal data; (ii) details about the purposes of the processing; (iii) information about the types of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the retention period for the data or the criteria used to determine it; (vi) information about the rights to erasure, rectification, restriction of processing,

and objection to processing; (vii) information about the right to lodge a complaint with the relevant data protection authority; (viii) if the data was not collected directly from the data subject, information about the source of the data; and (ix) information about the existence and explanation of any significant automated processing affecting the data subject. Additionally, the data subject can request a copy of the personal data being processed.

- **Right to rectification of errors**
  Data subjects have the right to request the rectification of inaccurate or incomplete personal data held by controllers. Controllers are responsible for ensuring that any inaccuracies or omissions in the data are promptly corrected or erased. The right to rectification empowers individuals to have their personal data updated, ensuring its accuracy and completeness. It is important for controllers to maintain mechanisms and processes to address such requests and take appropriate actions to rectify any errors. By exercising the right to rectification, data subjects can ensure that their personal data is up to date and reliable.
- **Right to deletion/right to be forgotten**
  Data subjects have the right to request the erasure of their personal data, commonly known as the "right to be forgotten" under certain circumstances. The right to erasure can be exercised if: (i) the data is no longer necessary for its original purpose, and there is no legitimate basis for its continued processing; (ii) the data subject provided consent for the processing, but subsequently withdraws that consent, and there are no other legal grounds for processing the data; (iii) the data subject exercises the right to object to the processing, and the controller does not have overriding legitimate reasons for further processing; (iv) the data has been processed unlawfully; or (v) erasure is necessary to comply with EU or national data protection laws.
  It is important to note that the right to erasure is not absolute and is subject to certain limitations. For instance, it may not apply if retaining the data is necessary for exercising the right of freedom of expression and information, compliance with a legal obligation, the performance of a task carried out in the public interest or the exercise of official authority, or the establishment, exercise, or defence of legal claims.
  Controllers must establish mechanisms and procedures to handle requests for erasure and ensure that personal data is securely and permanently deleted or anonymised. By exercising the right to erasure, data subjects can have their personal data removed from the controller's records, provided the conditions for erasure are met.
- **Right to object to processing**
  Data subjects have the right to object to the processing of their personal data if they can demonstrate specific reasons related to their situation. This right applies when the basis for the processing is either the public interest or the legitimate interest of the controller. Upon receiving such an objection, the controller must halt the processing of the data, unless it can present compelling legitimate grounds that outweigh the interests, rights, and freedoms of the data subject, or if the data is necessary for establishing, exercising, or defending legal rights.
  The right to object empowers individuals to have a say in how their personal data is processed, especially when it involves public or legitimate interests. Controllers must establish mechanisms to handle objections and assess the validity of the data subject's claims. If the controller cannot demonstrate compelling legitimate grounds, they must cease the processing of the personal data in question. However, if there are legitimate reasons for the processing that outweigh the data subject's interests, or if the data is required for legal purposes, the controller may continue the processing.
  This right provides data subjects with a means to protect their privacy and have control over the processing of their personal data, ensuring that their rights and freedoms are respected.
- **Right to restrict processing**
  Under the GDPR within the EU, data subjects have the right to request the restriction of the processing of their personal data. This means that the controller can only retain the data and use it for limited purposes under certain circumstances. The right to restrict processing applies in the following situations: (i) when the accuracy of the data is disputed, the data subject can request restriction until the accuracy is verified; (ii) if the processing of the data is unlawful, and the data subject chooses to request restriction instead of erasure; (iii) if the controller no longer needs the data for its original purpose, but it is still required by the controller to establish, exercise, or defend legal rights; or (iv) when the verification of overriding grounds is pending in the context of an erasure request.
  In these cases, the controller must comply with the data subject's request to restrict the processing of their personal data. This means that the data will be held but not further processed except for limited purposes, as specified by the data subject or as required for legal purposes. The right to restrict processing allows individuals to have more control over the use of their personal data and provides a mechanism to protect their rights while unresolved issues or disputes are being addressed.
  It is important for controllers to have procedures in place to handle requests for restricting processing and to ensure that the restricted data is securely stored and used only in accordance with the specified limitations.
- **Right to data portability**
  The right to data portability grants data subjects the right to obtain a copy of their personal data in a commonly used machine-readable format. This enables individuals to transfer their personal data from one data controller to another or have it transmitted directly between controllers, when technically feasible.
  By exercising the right to data portability, data subjects can have greater control over their personal data and facilitate the seamless movement of their information between different service providers or platforms. This right promotes individual empowerment and fosters competition and innovation in the digital landscape by enabling individuals to easily switch service providers and utilise their personal data across different platforms or systems.
  It is important to note that the right to data portability applies to personal data that individuals have provided to the controller based on their consent or for the performance of a contract. The data must be processed by automated means. Additionally, the right is subject to certain limitations and exceptions, including protection of the rights and freedoms of others and compatibility with applicable legal obligations.
  Controllers must ensure the technical and organisational capabilities to fulfil requests for data portability, enabling data subjects to exercise this right smoothly. By offering data portability options, organisations can enhance transparency, foster trust, and empower individuals to leverage their personal data in ways that suit their needs and preferences.
- **Right to withdraw consent**
  Data subjects have the right to revoke their consent at any time. The withdrawal of consent does not impact

the legality of the processing that was based on consent prior to its withdrawal. Before providing consent, the data subject must be informed about their right to withdraw consent. The process of withdrawing consent should be as simple and accessible as giving consent initially.

This right recognises the importance of individuals maintaining control over their personal data and allows them to make choices about the processing of their information. It ensures that data subjects are not bound indefinitely by their initial consent and have the freedom to change their preferences or restrict further processing.

It is important for organisations to respect and facilitate the withdrawal of consent. They should have clear mechanisms in place to handle withdrawal requests and promptly act upon them. By ensuring that the withdrawal process is easy and straightforward, organisations can uphold individuals' rights and promote transparency and trust in their data processing practices.

- **Right to object to marketing**

  The right to object to marketing allows data subjects to refuse the processing of their personal data for direct marketing purposes, including profiling. This right gives individuals control over receiving marketing communications and targeted offers based on their personal information.

- **Right protecting against solely automated decision-making and profiling**

  The right to protection against solely automated decision-making and profiling ensures that data subjects are not subjected to decisions that are based solely on automated processing, including profiling, and that have significant legal effects or similarly significant impacts on them. However, this right is subject to certain restrictions: (i) if the solely automated decision is necessary for entering into or performing a contract between the data subject and the controller; (ii) if the solely automated decision is authorised by EU or Member State law applicable to the controller, provided that suitable measures are in place to safeguard the rights of the data subject; and (iii) if the solely automated decision is based on the explicit consent of the data subject.

  This right protects individuals from unfair or discriminatory decision-making processes that rely solely on automated algorithms or profiling techniques. It ensures that human intervention or alternative means of decision-making are available when decisions have significant implications for the data subject. Exceptions exist when certain conditions, such as contractual necessity, legal authorisation, or explicit consent, are met.

  The purpose of this right is to safeguard individuals from potential adverse effects resulting from fully automated decisions and to provide them with the opportunity to have a say in decisions that significantly impact their lives.

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

  Data subjects have the right to file complaints regarding the processing of their personal data with the appropriate data protection authority in their jurisdiction. If data subjects reside in Cyprus or if the alleged violation of their rights occurred within Cyprus, they can seek recourse by lodging a complaint with the Commissioner. This right enables individuals to report concerns or alleged infringements related to the handling of their personal data and seek resolution from the relevant regulatory body.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The right for data subjects in Cyprus to mandate not-for-profit organisations for seeking remedies on their behalf or engaging in collective redress processes is provided under Article 80 of the GDPR. Article 80 specifically addresses the representation of data subjects and the empowerment of not-for-profit organisations to act on their behalf in matters related to data protection. It recognises the importance of collective actions and the role of organisations in advocating for data subjects' rights and seeking appropriate remedies.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

Where the provision of information society services directly to a child is based on the consent of the child, the processing of personal data is lawful if the child is at least 14 years old.

For a child under the age of 14 years old, the processing of personal data referred to in the previous paragraph is considered lawful following a consent given or authorised by the person who has parental responsibility for the child.

The controller must make reasonable efforts to verify that the consent has been given or authorised by the holder of parental responsibility in light of available technology. Given that children need specific protection, any information or communication, where processing is addressed to a child should be in a clear and plain language that the child can easily understand. The controller must ensure that the child is informed and understands what she/he consents to, otherwise the consent is not valid.

7 Registration Formalities and Prior Approval

7.1 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?

There is currently no requirement for organisations to register with or notify the Commissioner. However, in accordance with the GDPR, the controller entity must consult the Commissioner prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

7.2 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)?

This is not applicable in Cyprus.

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

This is not applicable in Cyprus.

7.4 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)?

This is not applicable in Cyprus.

7.5 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)?

This is not applicable in Cyprus.

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

This is not applicable in Cyprus.

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

This is not applicable in Cyprus.

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

This is not applicable in Cyprus.

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

This is not applicable in Cyprus.

7.10 Can the registration/notification be completed online?

This is not applicable in Cyprus.

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

This is not applicable in Cyprus.

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

This is not applicable in Cyprus.

8 Appointment of a Data Protection Officer

8.1 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 (**DPO**) is mandatory where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories or personal data relating to criminal convictions and offences.

The Commissioner may prepare and make public the list of processing operations and cases requiring the appointment of a DPO. So far, the Commissioner has not published such a list.

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

Infringements of the obligations of the controller and the processor pursuant to Article 37 (*designation of data protection officer*) of the GDPR are subject to administrative fines up to 10 million EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

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

Several safeguards exist in order to enable the DPO to act in an independent manner, one of them being that no dismissal or penalty can be issued by the controller for the performance of the DPO's tasks.

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

Yes, a group of entities may appoint a single DPO provided that he or she is "easily accessible from each establishment".

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

The GDPR requires that the DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39 of the GDPR.

The necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, where a data processing activity is particularly complex, or where a large amount of sensitive data is involved, the DPO may need a higher level of expertise and support.

The necessary skills and expertise include:

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR;
- understanding of the processing operations carried out;
- understanding of information technologies and data security;
- knowledge of the business sector and the organisation; and
- the ability to promote a data protection culture within the organisation.

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

The DPO is responsible for monitoring compliance with the Regulation within the Organisation. Their role is advisory. The main tasks are to inform the controller of their obligations and to provide advice on request as to when and how a data protection impact assessment should be carried out. The DPO is usually the contact point between the Organisation and the Office the Commissioner.

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

Yes, the controller or the processor must inform the Commissioner of the contact details of the designated DPO. The notification must be in writing and in Greek.

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

The DPO is not required to be named in a public-facing privacy notice or equivalent document, although the contact details of the DPO must be provided to the data subjects whose data are being processed to ensure communication.

9 Appointment of Processors

9.1 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?

Where processing is to be carried out on behalf of a controller, a contract or other legal act binding the processor to the controller must be in force.

9.2 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 agreement must be in writing and set out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

10 Marketing

10.1 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?).

Electronic direct marketing requires the clear, affirmative consent of the recipient which must be consistent with the definition of consent and any further conditions under the GDPR. In Cyprus, Law No. 112(I)/2004 (as amended) transposes the ePrivacy Directive and stipulates in part 14 (Article 106) that the use of automatic calling and communication systems without human intervention (automatic calling devices), facsimile devices (faxes) or e-mail for direct marketing purposes is permitted only in the case of subscribers or users who have given prior their consent. If a natural or legal person obtains from its customers their email contact details in the context of the sale of a product or service, in accordance with the provisions of the GDPR may use said data for the direct commercial promotion of its own similar products or services, provided that the its customers clearly and conspicuously have the opportunity to object, free of charge and easily, to this use of electronic contact details at the time of their collection, and this with each message, in case the user had not initially objected to this use.

The practice of sending e-mail messages for the purpose of direct commercial promotion, which disguises or conceals the identity of the sender or the person on whose behalf and/or for whose benefit the message is sent, is prohibited, or without a valid address at which the recipient can request the termination of this communication, or with which the recipients are encouraged to visit websites that violate this condition.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The limitations concerning personal data are specifically applicable to individuals and do not extend to legal entities. However, it is important to note that certain information identifying sole traders may be considered as personal data, and would thereby be subject to the applicable restrictions. Additionally, restrictions may also apply to marketing activities targeted at employees through their business email accounts. According to Cyprus Law No. 112(I)/2004 (as amended), if a natural or legal person obtains from its customers their email in the context of the sale of a product or service, in accordance with the provisions of Regulation (EU) 2016/679 and the Law, the natural or legal person may use said data for the direct marketing of its own similar products or services, provided that its customers have a clear and distinct opportunity to object, free of charge and easily, to this use of electronic contact information at the time of collection, and this opportunity is presented with each message, in case the user had not initially objected to this use.

10.3 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.).

Please see our answer to question 10.1 above.

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

The GDPR applies to organisations that are based in the EU even if the data is stored or processed outside the EU, and also to organisations that are not in the EU if one of the conditions for extraterritorial application set in the GDPR applies. Law No. 112(I)/2004 provides in Article 3 that the provisions of this law constitute the framework for the regulation of electronic communications networks and services and postal services provided by persons in the territory of the Republic of Cyprus.

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

The Commissioner usually follows up with complaints of data subjects or performs audits to entities, and the Commissioner has been active in the enforcement of breaches thereof.

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

Law No. 112(I)/2004 provides that personal data contained in printed or electronic subscriber lists, which are available to the public and/or can be obtained through directory information services, must be limited to what is necessary to identify the identity of a particular subscriber, unless the subscriber has given additional consent to the publication of additional personal data.

Telephone directory service providers must inform subscribers, free of charge, about the purposes and potential use of public directories, including personal data. Subscribers have the right to decide, at no cost, which personal data is included in public directories, as long as the necessary identifying information is provided. Subscribers can request and obtain, free of charge, verification, correction, or withdrawal of their personal data from the directories.

Directory service providers obtain the additional consent of subscribers before each addition of their personal data to the telephone directories, and before making available or using telephone directories for reverse or multiple search services.

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

The GDPR and Law No. 112(I)/2004 provide different sanctions. Law No. 112(I)/2004 provides that the Commissioner may impose administrative fine up to 200,000 EUR. The GDPR provides that administrative fines up to 20 million EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher, can be imposed for breach of basic principles of processing including conditions for consent.

11 Cookies

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

The use of cookies in Cyprus is regulated by the Law on the Regulation of Electronic Communications and Postal Services of 2004, L. 112(I)/2004 and the Law. Storing information or gaining access to already stored information in the terminal equipment of a subscriber or user is permitted only if the specific subscriber or user has given his consent, including for the purpose of processing:

Provided that any storage or access of a technical nature is not prevented, the sole purpose of which is to carry out the transmission of a communication, through an electronic communications network, or which is absolutely necessary for the service provider of the information society that the subscriber has expressly requested to be able to or the user to provide the specific service.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The applicable restrictions distinguish between two different types of cookies; namely, essential cookies do not require the user's consent as they are technically necessary for identification and retention of content entered by a user during a session on a website, presentation of the website and to connect the user to services that require authentications whereas third-party cookies require the user's consent as they are installed for online advertising, targeting and web analytics.

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

To date, the Commissioner has not taken any enforcement action in relation to cookies; although recently, the Commissioner focused on the lawful use of cookies and completed 30 audits regarding the use of cookies by news and public information websites. Therefore, the Commissioner may take enforcement actions soon.

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

In case of violation of cookie restrictions, according to Article 83(5) of the GDPR, the fine framework can be up to 20 million EUR, or in the case of an undertaking, up to 4% of their total global turnover of the preceding fiscal year, whichever is higher.

12 Restrictions on International Data Transfers

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

Where the controller or the processor intends to transmit specific categories of personal data to a third country or to an international organisation, such transfer can only take place if the transfer is made to a jurisdiction having an adequacy decision as specified by the European Commission, if there is one of the required safeguards as specified in the GDPR, or one of the derogations as specified in the GDPR applies to the transfer.

12.2 Please describe the mechanisms businesses 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, one of which 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: (i) controllers; (ii) processors; (iii) a controller (as exporter) and a processor (as importer); and (iv) a processor (as exporter) and a controller (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.

12.3 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.

Provided that personal data will be lawfully transferred to other jurisdictions with all appropriate safeguards on the data transfer in place, transfers do not require prior notification to the Commissioner.

12.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in Schrems II (Case C-311/18)?

The Commissioner has not issued any guidance on this topic.

12.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses published on 4 June 2021?

No guidance has been issued by the Commissioner.

13 Whistle-blower Hotlines

13.1 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 whistleblowing policies are generally established in order to implement proper corporate governance principles in the normal functioning of the businesses. Whistleblowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements businesses' regular information and reporting channels.

Whistleblowing legislation in Cyprus regulates reporting of breaches of EU and Cyprus law. Breaches of Cyprus law that may be reportable under the Whistleblowing law include:

(a) acts or omissions related to the commission or potential commission of a criminal offence, in particular, corruption offences;
(b) acts or omissions related to non-compliance with any legal obligation imposed on a person;
(c) infringements which endanger or are likely to endanger the safety or health of any person; and
(d) infringements that cause or are likely to cause damage to the environment.

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

The Law does not regulate anonymous reporting.

14 CCTV

14.1 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)?

People who are about to be videotaped must be informed of the videotaping and given the right to "refuse" to be videotaped by avoiding entering the building in which the videotaping takes place. The sign must be placed in a place outside the visual field or at a point before the cameras can record people. Furthermore, the signs must contain the information referred to in Article 13 of the GDPR or state that the area is being video monitored, with the information and contact details of the Data Controller and refer to the Privacy Notice link.

The size and location of signs depends on the circumstances. They must be visible and readable by people with moderate vision. They should not be hung in uncomfortable places or obscured by other visual obstacles. For example, if a sign needs to be placed higher than eye level, it needs to be larger and in larger letters to be read from below.

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

Yes, according to opinion 2/2018 of the Commissioner, any Community that wishes to invoke the provisions of Law 138(1)/2001, must be able to demonstrate that the need to use CCTV in a specific public space overrides the right to privacy of passers-by. Individual incidents of offences or vandalism in this area do not justify the use of CCTV. If these incidents occur systematically, the Community should first resort to less intrusive preventive measures, such as, for example, illumination of the space or the activation of the institution of the observer of the neighbourhood or the security guard employment. Communities should assess the impact that monitoring will have of a specific area with CCTV, in the neighbouring areas and in the wider areas. The use of CCTV in places where the commission of serious crimes is systematically observed, was justified only in cases where the Police, for essential reasons, did not provide adequate policing in this area. In the absence of legislative regulation, the use of CCTV in public places is allowed, only in exceptional cases where there is a compelling and justified overriding public interest and provided that there are no other less intrusive measures.

Furthermore, the Commissioner has given some guidelines for the operation of the CCTV based on the GDPR and Article 23(i) of the Law 138(I)/2001. To be able to use them, there must be a legal basis that allows the processing of personal data. Article 6 of the GDPR lists six legal bases for the legality of processing. The one that seems to apply in the case of the GDPR is (f) which allows the processing for the sake of "the protection of the legitimate interests pursued by the controller or a third party unless these interests are overridden by the interest or the fundamental rights and freedoms of the data subject that imposes the protection of personal data, in particular if the data subject is a child". This article gives the possibility to the owners of private premises to install and use CCTV invoking

the prevention, suppression of crimes or the legal interests they pursue (such as the protection of the premises). The above legal basis can be used to justify the video recording of private spaces. The justification for surveillance in public places, however, needs to be approached more carefully, as people in public places expect reasonable respect for their privacy. It is noted that those responsible for the operation of CCTV must be able to justify due to the invasive nature of the monitoring that there is no alternative, less invasive method to achieve their purpose. However, if the alternative method entails a disproportionate cost, this cost may be a decisive factor in evaluating the acceptability of using CCTV.

15 Employee Monitoring

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

Systematic monitoring of employees' activities, including the monitoring of the employees' workstation, internet activity and the use of GPS on employees' vehicles is subject to DPIA.

According to the Directive of the Commissioner for Personal Data Protection for the Processing of Personal Data In the Field of Labour Relations, the control and monitoring of employees in the workplace is allowed under the Law, given that the employer is able to justify the legality and necessity of the control and monitoring and that there is no other less intrusive way to proceed. The legitimate need of the employer, to be justified, must prevail over the rights, interests and fundamental freedoms of employees. Data such as the voice, image, email address and number work phone numbers that can identify an employee are their personal data. The data that are collected and processed through tracking systems/control that the employer has installed in the workplace must are used only for the purposes intended by the employer and they must be destroyed or deleted once these purposes have been fulfilled. If one employer uses outgoing telephone recording systems calls for billing purposes or closed-circuit video surveillance for the purpose of protecting the workplace from outsiders' interventions, they cannot use these systems for the purposes of monitoring employees during their breaks. For example, an employer who has installed video cameras for the protection of his premises during the night hours, cannot monitor the employees during their work during the day.

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

Employers should not use consent as the legal basis as EU supervisory authorities, including the Commissioner, do not generally consider consent given in the employment context as freely given and often consider it invalid. Consent must comply with GDPR Articles 7 (Conditions for consent) and 6(1)(a), which require data subjects to give consent for specified purposes.

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

According to the opinion 1/2018 of the Commissioner for personal data protection to all connections regarding notification by named employers statement with the salary and the amount of the contribution that is deductible by the employees, regarding members of associations, and referring to Articles 4 – 6, 13 and 14 of the GDPR and it concludes that the employer companies have the obligation to notify/provide a statement of the salary and the amount of the contribution deducted from each individual employee who is a member of the Trade Union, given the fact that: (a) the amounts in question are absolutely necessary for the Trade Union to be able to perform its duties based on Article 35 of the Trade Unions Law; and (b) the employees have been previously informed.

15.4 Are employers entitled to process information on an employee's COVID-19 vaccination status?

No. Employees only have the obligation to inform the employer that they underwent a test, and about its result, in order for the employer to draw up the weekly schedule that they must follow, based on the relevant Decrees of the Republic of Cyprus.

16 Data Security and Data Breach

16.1 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 manner that ensures appropriate security and confidentiality of the personal data against unlawful processing. Both controllers and processors are responsible for ensuring that the data are kept secure.

16.2 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.

As soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority in Cyprus (and other applicable supervisory authorities) without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The notification referred above shall include the following information:

(a) Description of the personal data breach, including the approximate number of affected data subjects and personal data records.
(b) Contact details of the DPO or other point of contact for obtaining more information.
(c) Explanation of the potential consequences resulting from the personal data breach.
(d) Description of the actions taken or planned by the controller to address the breach, including any measures to minimise its impact.

16.3 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 and, where feasible, not

later than 72 hours after having become aware of it, 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 DPO (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). In addition, the Law provides that the controller may be relieved, wholly or in part, of the responsibility for the disclosure of a personal data breach to the data subject for one or more of the purposes referred to in paragraph (1) of Article 23 of the GDPR.

16.4 What are the maximum penalties for data security breaches?

See question 17.1(d) below.

17 Enforcement and Sanctions

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

(a) **Investigative Powers:** In the exercise of his investigative powers, the Commissioner shall seize documents or electronic equipment under a search warrant in accordance with the provisions of the Criminal Procedure Law.

(b) **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).

(c) **Authorisation and Advisory Powers:** Advisory powers include advising the controller in accordance with the prior consultation procedure, to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data, to authorise processing, if the law of the Member State requires such prior authorisation, to issue an opinion and approve draft codes of conduct pursuant, to accredit certification bodies, to issue certifications and approve criteria of certification, to adopt standard data protection clauses and to authorise contractual clauses as well as to authorise administrative arrangements and to approve binding corporate rules.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions:** The GDPR provides for administrative fines which can be 20 million EUR or up to 4% of the business's worldwide annual turnover of the preceding financial year. No criminal sanctions apply. The Law provides that an administrative fine imposed on a public authority or public body for non-profit-making activities shall not exceed 200,000 EUR.

(e) **Non-compliance with a data protection authority:** The GDPR provides for administrative fines which will be 20 million EUR or up to 4% of the business's worldwide annual turnover of the preceding financial year, whichever is higher. No criminal sanctions apply. The Law provides that an administrative fine imposed on a public authority or public body for non-profit-making activities shall not exceed 200,000 EUR.

17.2 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 Commissioner to impose a temporary or definitive limitation including a ban on processing.

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

The Commissioner usually examines complaints from data subjects, and audits and issues warnings, reprimands or administrative fines. Recently, an administrative fine of 5,000 EUR on the complainee was imposed since it was decided by the Commissioner that complainee did not ensure, as it should have done, the protection of the complainant's personal data from unauthorised or unlawful processing nor had it taken adequate measures in advance to be able to prevent or detect the alleged infringement.

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

The Commissioner has not exercised its powers against businesses established in other jurisdictions so far.

18 E-discovery / Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

E-discovery requests are not regulated by a legal framework in Cyprus.

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

No guidance has been issued by the Commissioner.

19 Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Personal data breaches under the Law continue to constitute the majority of enforcement decisions issued by the Commissioner over the past 12 months. In the case of a complaint made to the Commissioner about a leak of personal data of a citizen to a third party, a citizen filed a complaint with the Office of the Commissioner, against a public authority in Cyprus (the Complainee), regarding a leak of his personal data to a third party. The leak concerned simple-category personal data, which was contained

in the Complainee's consent form, which instead of being given to the complainant himself, whom it concerned, was given to a third person.

As it emerged during the investigation, the Complainee did not ensure, as it should have done, the protection of the complainant's personal data from unauthorised or unlawful processing. Nor had it taken adequate measures in advance to be able to prevent or detect the alleged infringement. Therefore, finding a violation of Articles 5(1)(f), 24(1) and 32 of the Regulation, an administrative fine of 5,000 EUR on the Complainee was imposed.

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

A focus for Cyprus's Commissioner for Personal Data Protection is the lawful use of cookies and the Commissioner recently announced the completion of 30 audits regarding the use of cookies by news and public information websites.

Michael Kyriakides leads the Commercial & Corporate Litigation & Advisory at Harris Kyriakides. He advises on matters related to Data Privacy, GDPR and Cyprus Cyber Law compliance, software and hardware licensing, development, procurement, governance, e-commerce, information technology projects, data privacy and dispute resolution.

Harris Kyriakides
115 Faneromenis Avenue
Antouanettas Building
6031 Larnaca
Cyprus

Tel: +357 24 201 620
Email: m.kyriakides@harriskyriakides.law
URL: www.harriskyriakides.law

Eleni Neoptolemou is a Partner of the Commercial Team at Harris Kyriakides. Eleni specialises in the areas of oil and gas, administrative law, tender processes, and data protection. She regularly appears before the Administrative Court of Cyprus and other authorities, such as the Tenders Review Authority and Consumer Protection Service, and assists in cases challenging decisions of public authorities on behalf of private clients. She also provides opinions regarding oil and gas matters regarding legal and contractual matters. Eleni is a registered mediator for civil and commercial disputes.

Harris Kyriakides
1 Kinyra Street, 5th Floor
1102 Nicosia
Cyprus

Tel: +357 22 057 754
Email: e.neoptolemou@harriskyriakides.law
URL: www.harriskyriakides.law

Munevver Kasif is an Associate of the Commercial Department at Harris Kyriakides. She specialises in the areas of data protection, shipping, commercial and regulatory. She assists and advises on documents regarding intellectual property matters and relevant legal proceedings. She also advises clients regarding regulatory compliance of marketing campaigns.

Harris Kyriakides
1 Kinyra Street, 5th Floor
1102 Nicosia
Cyprus

Tel: +357 22 057 758
Email: m.kasif@harriskyriakides.law
URL: www.harriskyriakides.law

Harris Kyriakides was established in 1976 and offers the full range of corporate and commercial legal services. The firm has a substantial transactional and corporate practice with extensive international reach and client base range. It has consistently advised national and multinational corporations, financial institutions and governmental organisations and it maintains leading clients from several industries and business sectors, including banking, insurance, real estate, telecommunications, shipping, oil, construction, motor, tourism and leisure, pharmaceuticals, advertising, and others. The firm is highly ranked by various independent researchers and legal professionals and acknowledged in prestigious national and international directories and publications, including *The Legal 500*, *Who's Who Legal* and *Chambers and Partners*.

www.harriskyriakides.law

HARRIS KYRIAKIDES

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group