Cyprus

Andreas Neocleous & Co LLC
Nicholas Ktenas & Chrystalla Neophytou

1. LEGISLATION

1.1 Name/title of the law

The Processing of Personal Data (Protection of Individuals) Law of 2001 (the Law) came into force on 23 November 2001. The Law was introduced in the context of harmonisation with the European Data Protection legislation and amended in 2003 in order to align domestic legislation with Directive 95/46/EC of the European Parliament and the Council Decision of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Furthermore, the Constitution of the Republic of Cyprus, which was established in July 1960, provides for the following two provisions regarding privacy:

- Article 15 states that every person has the right to respect for his private and family life and that there shall be no interference with the exercise of this right, except such as is in accordance with the law and is necessary in the interests of the security of the Republic, constitutional order, public safety, public order, public health, public morals or the protection of the rights and liberties guaranteed by the Constitution to any person.
- Article 17 of the Constitution provides that every person has the right to respect for, and to the secrecy of, his correspondence and other communication, if such other communication is made through means not prohibited by law.

1.2 Pending legislation

On 15 September 2011 the Ministry of Interior submitted a proposed amendment to section 5 of the Law, which sets out the grounds for legitimate processing, to be considered by the Committee on Financial and Budgetary Affairs. The amendment provides that the processing of data without the consent of the data subjects is legitimate if it is necessary for state security; the defence of the state; public security; the prevention, examination, investigation and prosecution of breaches of criminal law or the code of conduct of the legally established professions; and to safeguard important economic and financial interests of a member state or the EU, including monetary, fiscal and tax issues. The discussion is at a very early stage and the opinions of the Cyprus data protection authority, the Office of the Commissioner for the Protection of Personal Data (Commissioner) or other interested parties have not yet been submitted to the House of

Representatives.

1.3 Scope of the law

1.3.1 The main players

- A 'data controller' is any person who determines the purpose and means of the processing of personal data.
- A 'data processor' is any person who processes personal data on behalf of the controller. Acting on behalf of someone means serving someone else's interests and recalls the legal concept of 'delegation'. In the case of data protection law, a processor is called to implement the instructions given by the data controller at least with regard to the purpose of the processing and the essential elements of the means.
- A 'data subject' is a natural person to whom the data refer and whose identity is known or can be directly or indirectly ascertained, in particular on the basis of his identity number or on the basis of one or more relevant elements which characterise his existence from a physical, biological, psychological, economic, cultural, political or social point of view.
- A 'third party' is any person other than the data subject, the data controller and the data processor and the persons who, under the direct supervision or on behalf of the controller, are authorised to process the personal data.

1.3.2 Types of data

'Personal data' or merely 'data' are defined under section 2 of the Law as 'all information which refers to a living data subject'. Anonymous data are not considered to be personal data.

According to the Commissioner, a simple email address, even though it may not disclose its owner's identity, as well as the online habits of a person that can create his profile, can constitute personal data.

'Sensitive data' are data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, participation in a union, club or trade union organisation, health, sexual life and sexual orientation, as well as anything relevant to criminal prosecutions or sentencing.

1.3.3 Types of acts/operations

The law applies to the processing of personal data wholly or partly by automated means, and to the processing by other means of personal data which form part of a filing system (any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis) or which are intended to form part of a filing system.

1.3.4 Exceptions

The Law does not apply to the processing of personal data performed by a natural person in the course of a purely personal or a household activity.

1.3.5 Geographical scope of application

The Law applies to any processing of personal data which is performed:

- by a controller established in the Republic of Cyprus or in place where Cyprus law applies by virtue of public or international law; or
- by a controller not established in the Republic of Cyprus who, for the purposes of the processing of personal data, makes use of means, automated or otherwise, situated in the Republic of Cyprus, unless such means are used for the purposes of transmission of data through the Republic of Cyprus. In such a case the controller must designate, by a written statement submitted to the Commissioner, a representative established in the Republic of Cyprus, who is vested with the rights and undertakes the obligations of the data controller, the latter not being discharged from any special liability.

2. DATA PROTECTION AUTHORITY

The Office of the Commissioner for the Protection of Personal Data
(*Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*)
Iasonos 1, 2nd floor 1082, Nicosia, Cyprus
P.O Box 23378
T: +357 22818456
F: +357 22304565
E: commissioner@dataprotection.gov.cy
Web: *www.dataprotection.gov.cy*

2.1 Role and tasks

The Commissioner is a public independent administrative authority and its primary objective is to apply the Law and to ensure that every individual's right to privacy is protected when personal data are processed.

2.2 Powers

The Commissioner has the following powers:

- to inspect and supervise data controllers on its own initiative or following a complaint;
- to issue recommendations and opinions;
- to provide information and guidelines to the public as to their rights and obligations under the Law;
- to impose administrative fines on data controllers if found in breach of the Law; and
- to authorise upon application various processing activities that comply with the Law.

2.3 Priorities

No specific priorities have been set by the Commissioner; rather its focus is on the application of the Law and compliance of all relevant parties with it.

3. LEGAL BASIS FOR DATA PROCESSING

Section 5 of the Law specifies that personal data may be processed only if the

data subject has unambiguously given his consent. Non-sensitive personal data may be processed without the data subject's consent for certain specified reasons.

On the Commissioner's recommendation the Council of Ministers may make special rules for the processing of the most common categories of processing and filing systems or where serious matters of public interest make it appropriate. No such rules have yet been published.

3.1 Consent

3.1.1 Definition

Consent of the data subject is defined as any freely given, express and specific indication of his wishes, clearly expressed and informed, by which the data subject, having been previously informed, consents to the processing of personal data concerning him. The Commissioner has also adopted the Article 29 Data Protection Working Party's Opinion on Consent (WP 187).

3.1.2 Form

In principle the Commissioner does not require consent to be given in a specific form.

Sensitive personal data may be processed provided that the data subject has given his explicit consent. However, if the consent of the data subject was obtained unlawfully or is contrary to morals, custom or a specific law, consent does not lift the prohibition.

3.1.3 In an employment relationship

Consent must be given freely. In an employment relationship it may be questioned whether the subordinate position of the employee allows consent to be truly 'free', but this question has not yet been tested in the courts.

3.2 Other legal grounds for data processing

Non-sensitive personal data may be processed without the data subject's consent for one or more of the following reasons:

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

The collection and processing of sensitive data are generally prohibited by the Law and allowed only if the data subject has given his explicit consent or otherwise if at least one of the following conditions is fulfilled:

- processing is necessary in order for the data controller to fulfil his obligations or carry out his duties in the field of employment law;
- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;
- processing is carried out by a foundation, association or other not-for-profit organisation which has political, philosophical, religious or trade union aims, and the processing relates solely to its members and other persons with whom the organisation has relations in order to attain its objectives. Such data may be communicated to third parties only if the data subject gives his consent;
- the processing relates solely to data which are made public by the data subject or are necessary for the establishment, exercise or defence of legal claims before the court;
- the data are medical data and processing is performed by a person providing health services by profession who has a duty of confidentiality or is subject to relevant codes of conduct, on condition that the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or the management of healthcare services;
- processing is necessary for the purposes of national security or criminal policy, and is performed by a service of the Republic of Cyprus or an organisation or foundation authorised for this purpose by a service of the Republic and relates to the detection of crimes, criminal convictions, security measures and investigation of potential terrorist offences;
- processing is performed solely for statistical, research, scientific and historical purposes, and all appropriate measures are taken for the protection of the data subjects; or
- processing is performed for journalistic purposes or in the framework of artistic expression as long as the right to privacy and family life is not violated.

With regard to employees' sensitive personal data, section 11 of the Employment Order issued by the Commissioner provides that the employer may maintain data concerning the previous convictions of the employee, such as traffic accidents committed by a professional driver. It also provides that the collection and processing of such data must be absolutely necessary for purposes connected to the employment relationship or where this is imposed by national legislation. Where the collection of such data is deemed necessary, employers must inform employees in advance of the purpose. In any event, the data collection must also be in accordance with section 10 of the Police Law (Law 73(I)/2004), which, *inter alia*, provides that the Head of Police shall issue a certificate concerning the employee's clean record stating any sentencing only following an application made by the employee/applicant or his duly authorised representative (eg, employer).

The Law empowers the Council of Ministers to issue regulations providing for the processing of sensitive personal data in cases other than those mentioned above, when there are important reasons of public interest. No such regulation has been issued to date.

3.3 Direct marketing and cookies

The Law specifies that personal data cannot be processed by anyone for the purposes of direct marketing or provision of such services, unless the data subject notifies his consent to the Commissioner in writing. The Commissioner keeps a register with the details of the identity of all these persons. The data controller must therefore consult the register before each processing and record in its filing system the persons included in the register.

The use of techniques such as the collection of cookies, web-bugs (files designed to trace web-visitors) or other technical methods that are not always obvious to the data subjects concerned and which allow website operators to create detailed profiles of visitors, according to their preferences and visits to web pages, third party advertisements and the like, is not essentially incompatible with the Law. However in order to make the use of such techniques legitimate, the website operator should always inform visitors of the intended use of their personal data and obtain their consent in relation to such use ('opt-in').

Directive 2002/58 on Privacy and Electronic Communications (the e-Privacy Directive) was transposed into national law in April 2004 in the Regulation of Electronic Communications and Postal Services Law of 2004, Law 112(I)/2004. The amendment to the e-Privacy Directive (Directive 2009/136/EC) has not yet been transposed into domestic law and no timetable has been announced for transposition. The Commissioner follows the guidelines set out in the Opinion of the Article 29 Data Protection Working Party on online behavioural advertising (WP 171).

3.4 Data quality requirements

Data controllers must ensure the fair and lawful processing of personal data. Personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a manner that is incompatible with those purposes.

Moreover, any personal data which are processed must be accurate, relevant and not excessive in relation to the purposes for which they are collected.

3.5 Outsourcing

The data controller may outsource the processing to a data processor. The data processor must possess appropriate qualifications and provide sufficient guarantees as regards technical knowledge and personal integrity for the protection of confidentiality. Regarding this issue, the Commissioner follows the principles set out in Opinion 3/2009 of the Article 29 Data Protection Working Party on the Draft Commission Decision on standard contractual

clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (data controller to data processor).

3.6 Email, internet and video monitoring

3.6.1 General rules

The individual's right to private life and privacy of communications is established under the Constitution (in Articles 15 and 17 respectively) as well as in Article 8 of the European Convention of Human Rights. The Law for the Protection of the Confidentiality of Private Communications (Surveillance of Telecommunications) of 1996 (Law 92(I)/1996) gives effect to Article 17 of the Constitution. It requires the Attorney General to obtain a court order before monitoring private communications. In 2006 an amendment to Article 17 of the Constitution empowered the Attorney General to authorise telephone tapping under certain conditions, and the police to monitor web logs, downloads and emails as admissible evidence for criminal investigations.

The monitoring of emails and internet use, including monitoring by employers, is subject to the provisions of the Law, which does, however, not contain any specific provisions in this respect. The Commissioner has also issued general guidelines to raise public awareness regarding the dangers and risks relating to personal data and use of the internet. The purpose of these guidelines was to enlighten the general public as to the issues of identity theft, spyware, spam emails and phishing, and the particular issues involved in blogging and of social networking.

Video surveillance is also subject to the general provisions of the Law and the Commissioner has issued a Directive on Video Surveillance to provide good practice guidance in relation to the application of the Law to this form of personal data processing.

The Directive distinguishes between two environments in which video surveillance may take place. The first is premises which are privately owned but are freely accessible to the public, such as banks, shops and football fields; the second is public places, such as roads and parks, where the public expects there to be greater respect for its private life.

The Directive recommends that, although not legally obliged to do so, people who are responsible for the operation of CCTV should consult with the Commissioner before installing their systems, and follow any guidance given by the Commissioner.

According to the Directive, operators of CCTV systems which record natural persons must be in a position to justify their action as if they were collecting any other personal data.

By the very nature of CCTV, obtaining the express consent of data subjects as a legal ground for the data processing is highly impractical. However, if CCTV is used for the purposes of fighting, identifying and investigating crime, prosecuting criminal offences, public safety, protection of premises, national defence or security, road traffic monitoring and the like, the data controller will usually be in a position to invoke one of the other legal grounds for data processing (see section 3.2 above).

The use of CCTV in private premises can usually be justified by the owners on the grounds of prevention or detection of crime, or protection of a legitimate interest such as the security of their property.

However, in order to justify monitoring in public places a more careful approach will be necessary. The persons responsible for the operation of CCTV systems in public places must be in a position to show that the monitoring is necessary and that the benefits outweigh any resulting harm to the rights, interests and basic freedoms of the persons concerned.

CCTV should be installed only where there is no other alternative, less intrusive method capable of achieving the same end at a comparable cost. In accordance with section 4 of the Law, images should only be retained for as long as necessary to achieve the purposes of the recording. The persons responsible for the operation of CCTV cameras should have in place a specific retention policy for the recording media and should be in a position to justify the reasons for the selected retention period.

The person responsible for the operation of a CCTV system must file a written notification with the Commissioner, in accordance with section 7 of the Law, unless it falls within one of the exemptions to the Law.

The persons who will be recorded must be informed about the recording and given the right to decline to enter the building or the public premises in which the recording takes place.

All appropriate technical and organisational measures should be taken to ensure the security and confidentiality of any recordings, which should be accessible only to those who really need to see them.

No third party should be given access to the media unless there is a legitimate reason. For example, where the public can assist in identifying a criminal or a victim then it may be permissible to give access to the media.

If the recording includes images of other persons, their characteristics must be disguised before the recording is shown to a data subject who has requested access to his data so as not to violate their rights.

Data subjects have the right to request that the recording concerning them is destroyed, not used or not shown, in part or in whole, where they believe that the recording has not been carried out in accordance with the Law.

3.6.2 Employment relationship

Employers must take all possible steps to distinguish between employees' work and personal activities and restrict any monitoring to those activities which relate to the performance of their duties. For instance, an employer can install a system to monitor websites visited by his employees and their emails to ensure that use of the internet is made for work-related and not personal reasons. However, an employer is not allowed to access personal emails of employees in any event but should instead inform his employees that use of the email for reasons which are not work-related from computers which are installed at the workplace is not allowed and will be penalised.

In particular, employers have to respect the Law for the Protection of the Confidentiality of Private Communications (Surveillance of Telecommunications) of 1996 which prohibits interception or monitoring

of private communications of any kind, except with the previous express consent of both the originator and the recipient of the communication, or the consent of one of them in the case of indecent, annoying or threatening phone calls.

Monitoring of business emails, fax, internet websites, tracking phone calls, recording phone calls, CCTV monitoring and GPS monitoring are allowed under the Law as long as the employer can show that the monitoring is legitimate and necessary and that there are no other less intrusive means of achieving the intended objectives. These objectives must be such as to take priority over the rights, interests and fundamental freedoms of employees.

Voice recordings, pictures, email addresses and phone numbers of employees, which constitute personal data, if gathered through monitoring systems installed by an employer in the workplace, may only be used for the specific purposes for which they were gathered and must be destroyed or deleted after these purposes have been accomplished. For example, an employer who uses a CCTV system to monitor workplaces for security reasons may not use these systems for the purposes of monitoring employees during their breaks.

Before an employer installs any monitoring system he must first examine whether the intended control and monitoring as well as the data to be collected are proportionate to the purpose he seeks to accomplish. For example, it may not be necessary to monitor all employees or all of their activities and communications. The employer must choose the lowest level of monitoring necessary to meet the required objectives, with minimum possible intrusion into the personal life of employees.

The employer must inform his employees in advance about the purpose, the means and the duration of the control and monitoring to be applied. It is good practice for the employer to adopt a written policy which determines the parameters for employees' use of telephones, computers, internet and other similar facilities provided by the employer for their use and the ways in which the employer will control or monitor their use. Secret monitoring or monitoring without prior notice is prohibited under any circumstances.

Employers wishing to install monitoring systems in the workplace are recommended to consult employees or their trade union or other representatives to discuss the intended methods and consequences of monitoring. There is no obligation to consult.

Before providing a business with analytical statements with numbers dialled, telecommunications providers will require written confirmation that all users have been duly informed about the sending of such statements to the employer. Furthermore, unless the employer has received the express consent of the employees, the service provider must delete the last three digits from every number.

4. INFORMATION OBLIGATIONS

4.1 Who

Data controllers are responsible for providing information to data subjects

regarding data relating to them.

4.2 What

The data controller must provide the following information to the data subject:

- the name and address of the data controller and his representative if any;
- the purpose of the data processing;
- the recipients or the categories of recipients of data
- the existence of the right of access and rectification of data;
- specific information that may be required based on the nature of the processing.

4.3 Exceptions

With the prior approval of the Commissioner, the data controller is exempt from providing information in the following circumstances:

- the data subject is already aware of the information;
- the processing is performed for statistical and historical purposes or for purposes of scientific research and it is impossible to inform the data subject;
- where disproportionate effort would be required in order to inform the data subject; or
- if the communication of data is provided by another law.

In addition, the Commissioner may wholly or partly exempt the data controller from the obligation to provide information if the collection of personal data is performed for the purposes of defence, national needs, or national security of the Republic of Cyprus or for the prevention, detection investigation and prosecution of criminal offences.

There is no obligation to inform where data are collected solely for journalistic purposes.

4.4 When

The Law provides that the data controller shall provide the information at the time of collection: that is, at the time when the data are recorded.

4.5 How

The Law provides that the information has to be given in an appropriate and an explicit way.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

The Law provides that every person has the right to know whether the personal data relating to him are or were processed. This information must be given in writing.

Furthermore, at the request of a data subject, the data controller is required to provide, without excessive delay and expense, the following information:

- all the personal data relating to him which have undergone processing, the recipients or the categories of recipients as well as the categories of data which are or are to be processed;
- the purposes of the processing, the recipients or the categories of recipients, as well as the categories of data which are or are to be processed;
- the progress of the processing since any previous notification;
- the logical process upon which every automated processing of data in relation to the data subject is based, in cases where personal data are used to evaluate certain aspects of the data subject's personality.

In relation to health data, the data controller has the discretion to choose to give indirect access to the personal data. In that case, a healthcare professional will have access to the data and will report to the data subject.

To exercise the right of access, the data subject must submit a signed and dated request to the data controller, accompanied by proof of identity. The request may be sent by any appropriate means of communication.

5.1.2 Exceptions

See section 4.3 above.

5.1.3 Deadline

The data controller must communicate the information requested without delay, and at the very latest within four weeks after receipt of the request. If the controller does not reply within this period or if the data subject is not satisfied with the reply, the data subject has the right to appeal to the Commissioner.

5.1.4 Charges

The data subject may not be charged for exercising his right to access.

5.2 Rectification

5.2.1 Right

Any data subject has the right to require the data controller to rectify any incorrect personal data relating to him.

5.2.2 Exceptions

None.

5.2.3 Deadline

The data controller must rectify the personal data within four weeks of receiving the data subject's request.

5.2.4 Charges

A charge of €20 is payable by the data subject to the Commissioner.

5.3 Erasure

5.3.1 Right

Any data subject has the right to require the erasure of all personal data relating to him if the data are incomplete or irrelevant with a view to the purpose of the processing, if the recording, disclosure or storage of the data is prohibited, or if the data have been stored for longer than necessary.

5.3.2 Exceptions
See section 4.3 above.

5.3.3 Deadline
The data controller must erase the personal data within four weeks starting from the submission of the data subject's request.

5.3.4 Charges
None.

5.4 Blocking
5.4.1 Right
Any data subject has the right to block any use of personal data relating to him under the same conditions as the right to erasure.

5.4.2 Exceptions
See section 4.3 above.

5.4.3 Deadline
The data controller must erase the personal data within four weeks of receiving the data subject's request.

5.4.4 Charges
None.

5.5 Objection
5.5.1 Right
The data subject has the right to object, at any time, on compelling legitimate grounds relating to his particular situation, to the processing of data relating to him.

5.5.2 Exceptions
None.

5.5.3 Deadline
The data controller must respond within four weeks of receiving the data subject's request.

5.5.4 Charges
The data subject will be charged €20 to exercise his or her right of access.

5.6 Automated individual decisions

5.6.1 Right

A decision producing legal effects for a data subject, or materially affecting him, cannot be taken purely on the basis of automated data processing aimed at evaluating certain aspects of his personality.

In the case of such an automated decision, the data subject has the right to be informed about the logic involved in any automated processing of data related to him.

5.6.2 Exceptions

The Law does not provide for any exceptions.

5.6.3 Deadline

There is no deadline.

5.6.4 Charges

The data subject may not be charged for exercising this right.

6. REGISTRATION OBLIGATIONS

6.1 Notification requirements

6.1.1 Who

Data controllers must notify the Commissioner in writing about the establishment and operation of a filing system or the commencement of processing. Responsibility for notification lies with the data controller.

6.1.2 What

Any type of automated or semi-automated (and in some cases manual) processing must be notified to the Commissioner.

6.1.3 Exceptions

The controller is discharged from the obligation to notify in the following circumstances:

- Processing is performed solely for purposes directly connected with the work to be done and is necessary for the fulfilment of a legal obligation or the performance of a contract, and the data subject has been previously informed.
- The processing concerns customers or suppliers of the data subject and the data are neither transferred nor communicated to third parties.
- Processing is performed by a society, association, company, political party or similar body and concerns data related to their members, who have given their prior consent, and the data are neither transferred nor communicated to third parties.
- Processing is performed by doctors or other persons who provide health services and concerns medical data, provided that the data controller is bound by medical confidentiality or any other kind of confidentiality required by law or code of conduct, and the data are neither transferred

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

6.1.4 When
The Law does not specify when notification has to be made, but it is generally accepted that notification must be made prior to starting any automated processing activity.

6.1.5 How
The data controller is required to complete a paper copy of the standard notification form in Greek and submit it, together with the relevant fee, to the Commissioner. The standard notification forms are available on the website of the Commissioner. They include:
- the name and address of the controller and of his representative, if any;
- the purpose or purposes of the processing;
- a description of the category or categories of data subject and of the data or categories of data relating to them;
- the recipients or categories of recipient to whom the data might be disclosed;
- proposed transfers of data to third countries;
- a general description of the measures taken to ensure security of processing, in sufficient detail to allow a preliminary assessment to be made of their appropriateness and adequacy.

The Commissioner may require the notifying data controller to provide further information, for instance, regarding the origin of the personal data, the choice of automation technology and the security measures that are in place.

6.1.6 Notification fees
The notification fee is €50.

6.2 Authorisation requirements
6.2.1 Who
No authorisation is required to begin processing personal data. However, data controllers must obtain authorisation for data transfers.

6.2.2 What
Authorisation is required for the transfer of personal data to a country outside the European Economic Area (EEA).

6.2.3 Exceptions
None.

6.2.4 When

No transfer can be made until the application has been approved. Therefore the application must be made in good time. Periodic renewal is not required.

6.2.5 How

The data controller is required to complete a paper copy of the standard notification form in Greek and submit it to the Commissioner accompanied by any relevant documents such as consents, proof of the US 'safe harbour' registration, binding corporate rules or standard contractual clauses and the relevant fee. The requisite forms are available on the website of the Data Protection Commissioner.

6.2.6 Authorisation fees

The authorisation fee is €50.

6.3 Other registration requirements

Section 8 of the Law requires combinations of filing systems to be notified to the Commissioner by a statement submitted jointly by the controllers or by the controller who will combine two or more filing systems which are established for different purposes. 'Combination' means a form of processing which involves the possibility of connection of the data of one filing system with the data of a filing system or systems kept by another controller or other controllers or kept by the same controller for another purpose.

6.4 Register

The Commissioner maintains the following registers under the Law:

- a register of filing systems and processing notified to the Commissioner;
- a register of statements and authorisations issued by the Commissioner for the combination of filing systems;
- a register of persons not wishing to be included in filing systems which promote direct marketing or provision of services;
- a register of authorisations issued for the international transfer of personal data;
- a register of confidential filing systems, namely those systems maintained by the Ministers of Justice and Public Order and Defence and the Public Information Office, for the purposes of national security or the detection of particularly serious crimes. Combinations with at least one of these filing systems must also be registered in the register of Confidential Filing Systems.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

This role is not recognised under the Law and this is not a common role in Cyprus.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

The transfer or 'transmission' of personal data in itself is an activity which falls within the definition of 'processing of personal data' as provided under section 2 of the Law.

Under section 9 of the Law the transfer of processed data or of data which will be processed when they are transferred to another country outside the EEA may take place only on the basis of an authorisation issued by the Commissioner, who will issue an authorisation only if he is satisfied that the country concerned ensures a sufficient level of protection.

8.2 Legal basis for international data transfers

Personal data may, with the Commissioner's prior approval, be transferred on the basis of satisfactory data transfer agreements or binding corporate rules or under the US 'safe harbour' scheme.

8.2.1 Data transfer agreements

There is a general obligation under Law 138(1)/2001 for the data controller to notify the Commissioner in writing about international transfers of personal data.

The data controller is discharged from the obligation to submit a notification to the Commissioner in cases where a transfer is performed solely for purposes directly connected with the work to be done and is necessary for the fulfilment of a legal obligation or for the performance of a contract, provided that the data subject has been previously informed. However, this does not apply to insurance companies, pharmaceutical companies, data provider companies such as providers of financial and stock market information and financial institutions, such as banks and credit card issuers.

8.2.2 Standard contractual clauses

The Commissioner will issue an authorisation if he is satisfied that the contractual arrangements between the data exporter and the third country recipient satisfactorily ensure the protection of private life and fundamental rights of the data subjects. This is typically achieved by using the 'standard contractual clauses' approved by the European Commission. Draft contracts, including those based on the standard contractual clauses, must be submitted to the Commissioner for approval. It should be noted that the standard contractual clauses are not necessary if the proposed transfer is to a recipient in a country that has been recognised by the European Commission as providing adequate protection of data.

8.2.3 Binding corporate rules

Binding corporate rules (BCRs) are internal rules adopted by multinational groups to define the group's global policy with regard to international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection. Draft rules must be submitted to the Commissioner for approval together with a completed application form (available on the Commissioner's website). Cyprus participates in the mutual recognition procedure launched in

October 2008 by the Article 29 Working Party.

8.2.4 Safe Harbour

Data export may be authorised if the proposed data recipient is based in the US and participates in the 'safe harbour' self-certification scheme. However, participation is only one of the parameters considered by the Commissioner.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

The Law provides that the processing of data is confidential and that it may be carried out only by persons acting under the authority of the data controller or the data processor and only upon instructions from the data controller.

In cases where the data controller delegates the processing to others, the data controller must select data processors who possess appropriate qualifications and who provide sufficient guarantees as regards technical knowledge and personal integrity so as to ensure that confidentiality of the data will be maintained.

9.2 Security requirements

The Law provides that the data controller must take the appropriate organisational and technical measures for the security of data and their protection against accidental and unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing. Such measures must provide a level of security which is appropriate to the risks involved in the processing and the nature of the data processed.

9.3 Data security breach notification obligation

There is no obligation under Cyprus law to notify personal data security breaches to the data subjects concerned or to the Commissioner. Furthermore, the Commissioner has not issued any recommendation on this matter to date.

9.4 Data protection impact assessments and audits

There is no legal obligation under Cyprus law to carry out data protection impact assessments and audits.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY

10.1 Enforcement action

The Commissioner may adopt and issue opinions and make recommendations on his own initiative on any matter relating to the application of the fundamental principles of the protection of privacy and personal data.

The Commissioner can also issue an opinion on the merits of a complaint, which may contain recommendations for the controller. Furthermore either on his own initiative or in response to a complaint, the Commissioner may conduct an administrative inquiry into any filing

system. For this purpose the Commissioner has the right of access to personal data and to collect any requisite information, with only a few, limited exceptions.

10.2 Sanctions

In case of breach of the Law the Commissioner may impose the following administrative sanctions:

- a warning with a specific time-limit for rectification of the contravention;
- a fine of up to €10,000;
- temporary revocation of an authorisation;
- the destruction of a filing system or the cessation of processing and the destruction of the relevant data.

Fines imposed by the Commissioner may be collected as a civil debt.

Contravention of the Law by a person responsible for processing, with intent to obtain an unlawful financial benefit for the perpetrator or anyone else, or to cause injury to a third party, is punishable on conviction by imprisonment for up to five years, a fine of up to €10,000 or both. The same sanction applies if the breach of the Law endangers the free functioning of the government of the Republic of Cyprus or national security.

The Data Protection Commissioner does not issue reports on enforcement actions or penalties.

10.3 Examples of recent enforcement of data protection rules

The Data Protection Commissioner's website gives details of complaints received and how they were dealt with. For the first half of 2011 details regarding four complaints have been published. In one of the cases, relating to the transfer of information on court judgments to a credit information bureau, the Commissioner found no breach of the law. In a case regarding the recording of telephone conversations by an insurance company the Commissioner ordered the company to make clear from the outset that calls would be recorded. The third case related to loss of medical records in a state hospital. The Commissioner found that there had been a breach of the requirement to take appropriate measures to safeguard data under section 10(3) of the Law and imposed an administrative fine of €1,500, taking into account that the hospital concerned had no record of previous breaches. The final complaint, regarding a social networking site, was transferred to the UK authorities when the site owner relocated there.

The largest fine imposed by the Commissioner to date is €8,000. This was in respect of a case in 2009 involving the sending of unsolicited text messages. The large number of complaints received, the fact that the sender did not cooperate and that he had previously been fined in respect of similar breaches were all taken into account in setting the fine.

10.4 Judicial remedies

Every person has the right to apply to the competent court for the immediate suspension or non-performance of an act or decision affecting

him, which has been done or made by an administrative authority or a public or private corporate body, a union of persons or a natural person by processing of data, where such processing aims to evaluate certain personal aspects relating to him and in particular, his efficiency at work, his financial solvency, his credibility and his behaviour in general. Action may be taken under the Courts of Justice Law, the Civil Procedure Law or any other law which provides for the issue of provisional orders.

Moreover, a person suffering any harm as a consequence of acts infringing the provisions of the Law can initiate a civil action for damages. There is no published case law, because such cases (if any) would be dealt with in the district courts, the decisions of which are not routinely reported.

10.5 Class actions

Class actions are not permitted under Cyprus law.

10.6 Liability

Data controllers are liable for any damage resulting from breaches of the Law. Data subjects that have incurred damage from an action in violation of the Law may claim damages from the data controller. The controller will not be liable if he proves that the act which caused the damage cannot be assigned to him.