Complying with data protection legislation

May 02, 2014

Back in 2001, Cyprus implemented the data protection law in order to be in compliance with the EU legal framework at that time.

Data protection legislation, which is considered an important component of EU privacy and human rights law, aims to protect the rights and freedoms of persons when data are processed (regardless of whether such processing is automated (e.g. database) or it is intended to be part of non-automated filing systems (traditional paper files)) as well as to facilitate the free movement of such data.

In the words of the European Commission, the establishment and functioning of an internal market in which the free movement of goods, persons, services and capital is ensured requires not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded. Thus, data-processing systems shall respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals. In serving this purpose, economic and social progress must be ensured by common action in order to eliminate the barriers which divide Europe.

For the purposes of familiarising ourselves with the legal framework, a short analysis will be provided below in respect of the main definitions of the law followed by a summary of its main provisions and answers to various FAQ's at the end.

What is "personal data" under the law?

Personal data means any information of whatsoever nature relating to an identifiable natural person. Examples include a person's address, criminal record, credit card number and bank statements.

Who is a "controller" for the purposes of the law?

Data controllers are the people or bodies which determine the purposes and the means ofprocessing personal data (for the meaning of "processing" - see below). A controller may be an individual or a corporate/unincorporated body of persons. For instance, a medical practitioner would usually be the controller of the data processed on his clients or a football club would control the data processed on its members and the same applies with a telecommunication service provider controlling data of its clients. Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.

What is the meaning of "processing"?

Processing of persona data is a very wide term and means any operation(s) which is performed upon personal data, whether or not by automated means; this includes collection, recording, organisation, storage, adaptation or alteration, consultation, use, disclosure, transmission or otherwise making available, blocking, erasure or destruction of personal data. It is worth mentioning that retention of data (i.e. simply holding data) is also a form of "processing".

Who is a "data subject"?

Data subject means an individual who is the subject of personal data, i.e. from the examples mentioned above, a patient whose data are being processed by his medical practitioner, an employee whose data are being processed from the company to which he is employed to another company (for instance, this might happen in the process of negotiations for the acquisition of the one company by the other) or simply an internet user.

Who is a "processor"?

Processor is an individual or a company, public authority, agency or any other body which is assigned by the controller to process data on its behalf for a particular purpose. An example of a processor would be a marketing company which is assigned by a cars' import company to carry out a customer's satisfaction survey on its behalf. In other words, a processor "processes" personal data on behalf of the controller. Examples include accounting companies, call centres and payroll companies.

What is the aim of the law?

The law aims to protect the rights and freedoms of persons with respect to processing of personal data by laying down the principles determining when this processing is lawful. These rules relate to:

- the quality of data, i.e. data must be processed fairly and lawfully, and collected for specified and legitimate purposes and at the same be accurate (and up to date); and

- the legitimacy of data processing, i.e. data may be processed only if at least one of the conditions (specified below) has been met.

An obligation is also placed on the data controller to provide the data subject from whom data are collected with certain information relating to himself (i.e. the identity of the controller, the purposes of collecting such information, the potential recipients of the data etc).

In addition, the data subject has a right of access to the data. Significantly, the data subject may obtain from the controller confirmation as to whether or not data relating to him are being processed and may also obtain from the controller the rectification,

erasure or blocking of data the processing of which does not comply with the provisions of the law.

Sensitive data

Very stringent rules apply to the processing of sensitive data (data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, data concerning health or sexual preferences, data relating to criminal prosecution and criminal convictions). As a general rule, such data cannot be processed with derogation to be tolerated only in the exceptional cases stipulated by the law (e.g. when processing is mandated by the law).

Your Firm and the data protection law

All businesses that keep any information on living and identifiable people must comply with the data protection legislation. Below, a number of FAQ's will be answered for the purpose of highlighting certain areas of danger and providing readers with answers on topics of common interest including on transfers of data to countries outside Cyprus.

Do I need the data subject's consent (e.g. employee) in order to process data? Are there any exceptions for obtaining consent? For instance, does a company need to obtain the employee's consent before providing the employee's personal details to the company's accountant?

Processing of data is permitted only when a data subject has given its consent to such processing. Processing of data without the subject's consent is also permitted: 1) for the performance of a contract to which the data subject is party or; 2) for compliance with a legal obligation to which the controller is subject or; 3) to protect the vital interest of the data subject or; 4) to perform a task carried out in the public interest or; 5) for the purposes of the legitimate interests pursued by the controller or a third party's to which the data communicated. In the above example, it is therefore advisable that consent be obtained from the employee (it is very unlikely that an employee will refuse to give consent in such situations involving the transfer of data to lawyers, accountants etc.);

It is important to mention here that employers should be very careful when collecting an employee's consent because enforced consent does not constitute a "lawful" consent. Consent shall be freely given and shall be a specific and informed indication of the employee's wishes.

Are there any other conditions applicable?

Apart from the satisfaction of at least one of the above conditions, both before and during the communication of a data to a third party, this data must have been lawfully collected and further processed in accordance with the law. An example where this rule might be breached is the collection of excessive information from a data subject. Whilst a person visiting a website of a cinema theatre, it will be considered excessive

if he is asked to provide general information about himself (concerning his date of birth, place of birth, marital status etc.) in order to gain access at the website. Another example is when a person has provided certain information about himself (such as name, telephone number, email, date/place of birth, profession, etc.) for insurance purposes at a particular company. Whilst explicit consent may have been obtained by the said company and such data may lawfully be processed, nevertheless, if at a later stage the insurance company lists that person at the company's website as a "happy" customer, processing will no longer be lawful. Likewise, if the same company transfers various data collected from the said person to affiliate companies (such as banks) and as a consequence various emails/letters/offers are sent to the said individual, then again the use (processing) of the collected information will not be lawful (as the information has been collected by the insurance company for different purposes).

Does the data protection law apply to data transfers on the Internet?

Yes, a vast amount of information is transmitted through the internet and therefore, such an important means could not be exempt.

Is an employer permitted to install a closed circuit television (CCTV) for the better control of his employees?

The control and the supervision of employees at workplace is only allowed if there is no other less restrictive way for the performance of the above task pursued by the employer. The particular locations where CCTV's may be installed and the manner of recording and obtaining data shall be such so that no more data is collected other than what is reasonably necessary for the fulfilment of the objectives pursued by the employer (e.g. for the protection of the workplace from robberies and/or burglaries). In other words, an employer is not permitted to control the behaviour or effectiveness of the employees via such systems (such as CCTV's). Unless an exception applies under the legislation (e.g. protection of the State's defence), a relevant notice/sign that the premises are monitored by a CCTV shall be placed at an easily identifiable location (persons with an average level of visibility shall be able to read the wording of the notice) outside the area which is monitored by the CCTV so that a person may elect not to enter the premises.

Is an employer permitted to have access to employee's emails and/or monitor the phone calls made by them?

Whilst the main email address of particular company is not generally considered as personal data (e.g. info@institution.com), nevertheless, a personal account which is used solely and exclusively by an employee for his work (such as andreas.georgiou@institution.com) and at which the employee uses his own personal username and password to gain access, constitute personal data. In such case, the employee is entitled to expect that no one will use (legitimately) this account, unless otherwise informed by the employer (in certain cases the employer may have access to the content of an email – e.g. when it is opened at the presence of the employee). The employer may also record the time, date and the recipient of an email sent by an

employee. An employer is not allowed to monitor telephone calls made or received by employees; however, he may be entitled to receive detailed phone calls' statements from the relevant authority provided that the employees have been informed and consented to this (and such consent is presented to the relevant authority).

In which countries can data be freely processed?

Data may be transferred freely to another country which is a member of the European Union as well as to countries of the European Economic area. However, data transferred to third countries outside the EU or the European Economic area do require the Commissioner's prior permission. The Commissioner will grant permission if the other country provides an adequate level of protection (there is a list of the countries which are considered adequate) or if data is transferred to a US based organisation which is covered by the Safe Harbour commitments. In exceptional cases, the Commissioner may also grant permission for a transfer to a third country which does not provide an adequate level of protection if certain conditions are fulfilled.

Can data be transferred (to a country that does not provide adequate level of protection) between companies belonging to the same multinational group?

As stated above, for all transfers of data to countries non-members of the EU and the European Economic area, the permission of the Commissioner is required. If the transfer will be between companies belonging to the same multinational group, it is common for such corporations to adopt "binding corporate rules". These rules are essentially a global code of practice based on European standards and as long as they incorporate the essential principles, it is very likely that the Commissioner will grant permission to such transfer. It must be pointed out that binding corporate rules are only suitable to regulate intra-group transfers of data to companies (worldwide).

When a company wishes to transfer data to an organisation based in a third country that does not provide an adequate level of protection, a condition for obtaining permission for this transfer could be the adoption of the "standard contractual clauses". These clauses are basically a contract between the data exporter and the data importer which bind the latter to process the transferred data in accordance with the data exporter's domestic law. The European Commission has adopted three types of standard contractual clauses to facilitate transfers of data (in the above situation) which are, consequently, recognised by member States to facilitate adequate safeguards. Although at some Member States there is no need for prior authorisation in order to proceed with the transfer, nevertheless, as explained above, Cyprus maintains a licensing system. The Commissioner will examine an application for the issuance of a license to transfer data to a third country on a case by case basis taking into account the level of protection in that country and/or the contractual clauses and/or the binding corporate rules.

Conclusion

The general impression is that the institution of the data protection Commissioner has proved very helpful in Cyprus. The Commissioner's office is willing to address promptly any questions or issues which may be submitted for clarification or interpretation from time to time. Furthermore, various guidelines published by the Commissioner provide an excellent overview/background of the complex legislation in a reader friendly manner. Therefore, considering the above, a person having a business can easily identify whether further legal advice/measures need to be initiated so as to be in compliance with his data protection duties. What comes with surprise, however, is that in Cyprus, only very few companies/businesses comply with their obligations imposed by the legislation. Given the fact that the Commissioner is entrusted with significant powers and may impose heavy penalties, its relaxed approach taken so far towards individuals/corporations contravening the law, may change within the next years.

This content is solely for general information purposes. None of the information herein should be relied on or substituted for specific professional advice regarding a particular matter or situation and no person should act or refrain from acting on the basis of the information contained in this brochure without first obtaining advice from an attorney. A.G. Erotocritou LLC is not engaged in rendering legal services or advice by providing the information contained in this brochure. © A.G. Erotocritou LLC, a Cyprus lawyers' limited liability company regulated by the Cyprus Bar Association, with registration number HE 326006. Address: 1 Arch. Kyprianou and Ayiou Andreou Str, Loucaides Building, 6th floor, 3036 Limassol Cyprus

I Website: www.erotocritou.com I Telephone: +35725370101 I Fax: +35725370102 I
Email: info@erotocritou.com