

**COMMERCIAL COURIER**  
**LEGAL DEVELOPMENTS AFFECTING YOUR BUSINESS**

*This column looks at new laws and regulations which will have an impact on your business.*

## **PROTECTING YOURSELF ... FROM DATA PROTECTION**

*by Dr. Frank Chetcuti Dimech\**

\*Partner, CDF Advocates (<http://www.cdf.com.mt> - Telephone 21223334, Mobile 79223334, Fax 21248594, e-mail: [fcd@cdf.com.mt](mailto:fcd@cdf.com.mt)). CDF Advocates specialise in commercial law, company law, financial services, taxation, telecommunications, privatisation and alignment with EU law. This article is for information purposes and must not be relied upon as advice.

### ***Introduction***

The Data Protection Act is intended to implement the EU Data Protection Directive 1995 (95/46/EC) into Maltese law. Part 8 of the Act, which establishes the office of the Data Protection Commissioner, came into force on the 22<sup>nd</sup> March 2002, and in all probability the rest of the Act will come into force later on this year. Professor John Mamo has been appointed as the Data Protection Commissioner.

In a nutshell, the scope of the Data Protection Act is to protect each individual's right to privacy with respect to the processing of personal data. Whether we are conscious of it or not, each business in Malta probably has in its possession, to a greater or lesser degree, information about individuals, usually the customers of the business. The Act addresses the issue of how that information can or cannot be used ("processing"), and what measures have to be taken to ensure that such information is kept safely.

The Act does not define the items of information which constitute "personal data". Instead, "personal data" means any information relating to an identified or identifiable natural person, and an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Therefore if the information in one's possession allows the identification of an individual, that information is personal data and falls under the Act's protection. The most obvious "identifiers" would be name, surname, address, identity card number or e-mail address, but of course there are many other "factors" which enable identification. Some factors are given special treatment: personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life are classified as "sensitive personal data" and such data may only be processed with the explicit consent of the individual.

### ***Principles of Processing of Personal Data***

The Act refers to individuals as "data subjects", and the person who holds data about individuals is referred to as a "controller" of personal data. The controller must ensure that:

- 1) personal data is processed only if it is lawful;

- 2) personal data is always processed in a correct manner and in accordance with good practice;
- 3) personal data is only collected for specific, explicitly stated and legitimate purposes;
- 4) personal data is not processed for any purpose that is incompatible with that for which the information is collected;
- 5) personal data that is processed is adequate and relevant in relation to the purposes of the processing;
- 6) no more personal data is processed than is necessary having regard to the purposes of the processing;
- 7) personal data that is processed is correct and, if necessary, up to date;
- 8) all reasonable measures are taken to complete, correct, block or erase data, having regard to the purposes for which they are processed;
- 9) personal data is not kept for a longer period than is necessary, having regard to the purposes for which they are processed.

The link to the purpose specified at the point of collection is fundamental. Customers must be clearly told the purpose for which they are being requested to provide personal data, and subsequent use of that data must be in conformity with that declared purpose. Purposes determined after collection are likely to be in breach of the Act unless necessary steps are taken by the Controller (e.g. to seek the consent of the data subject for the new purpose).

This means that data collected by a business, for example in an application form for a service, or on a delivery note, or even in a newspaper crossword competition, may only be used for the purpose it was collected at that stage, which, to continue the example, would be to identify the customer for the purposes of providing the service and billing, or to effect delivery at the right address, invoice and provide subsequent maintenance, or to contact the lucky winner of the competition. Therefore using that data to provide information about other products and services, whether provided by the “controller” of the data or by third parties, or worse still, selling the data to a mass mailing list or e-mail spammers, is definitely not allowed.

Therefore the Data Protection Act seems to deal a heavy blow to the modern theories of cross-selling and one-to-one marketing. However not all is lost. As long as the customer is informed that the data he is being asked to supply may be used for other - specific, explicitly stated and legitimate – purposes, your marketing manager may turn back into the happy man you were so pleased with a few minutes ago.

The requirement of “lawfulness” of processing can be a cause of concern especially for organisations in the financial services industry. Does "lawfully" mean "lawfully under the Data Protection Act" or "lawfully under the laws of Malta"? So, for example, the Act allows, subject to certain conditions, the disclosure of personal data to third parties, but this would be unlawful under the Professional Secrecy Act if that data is confidential information. Similarly, the Act makes no restriction on internal communication of data within an organisation. However it is unlawful under the Professional Secrecy Act for one employee to disclose customer information to another employee of the same organisation unless the latter requires that information in order to provide a service requested by the customer. Therefore a situation may exist where notwithstanding the fact that data has been processed in accordance with the Data Protection Act, access to that data may still be restricted by the rules of the Professional Secrecy Act.

Accuracy of the data held is a principle which will send a shiver down the spine of most controllers of personal data. How often are you still sent mail at your old address, or addressed with your maiden surname after you got married, or receive mail addressed to a now deceased member of your family? Marketing professionals do their best to have their data as accurate as possible so that the message hits the right person – but now individuals will have the right to hit

back if your data about them is inaccurate. Your marketing manager and your legal counsel will see eye to eye for this time only, and agree to conduct a thorough clean-up of your once-trusted mailing list.

Those interested merely in historical, statistical or scientific processing of data will be pleased by the fact that they can hold on to the personal data for a longer period than is strictly necessary. For other purposes the data must be destroyed as soon as the purpose has been reached.

### ***When can you process personal data?***

Assuming that the controller of personal data can hand on heart declare that he has followed all the nine principles mentioned above and so the data is accurate and the purpose for processing known, it is then necessary to consider whether the law allows the processing or not. There are six scenarios under which personal data may be processed.

#### *1. if the data subject has unambiguously given his consent.*

Since there must, by definition, be an 'indication' of consent, implied consent (i.e. when consent is assumed in the absence of an indication) is unlikely to meet this requirement. It is interesting to note that while this subsection uses "unambiguously", Section 12(2)(a) dealing with sensitive personal data uses "explicitly". The difference between the two phrases is unclear since at any rate only written evidence can satisfy both tests. The individual may revoke his consent at any time. If the individual has not given his consent to the processing, the processing is only allowed if it falls under one of the other five headings.

#### *2. if it enables the performance of a contract with the data subject or enables measures that the data subject has requested to be taken before a contract is entered into.*

Therefore processing in order to provide a product or service requested by you customer is perfectly permissible, and no further consent is needed.

#### *3. if the controller of personal data has to comply with a legal obligation.*

This covers processing due to statutory duties imposed, by law, on controllers, e.g. reporting to the tax authorities or, for those in financial services, reporting of suspicious transactions under the Prevention of Money Laundering Regulations.

#### *4. in order to protect the vital interests of the data subject;*

The Act, unlike the EU Directive, does not define "vital interests". It seems that "vital interests" should involve some kind of emergency; the preamble to the Directive cites the protection of "an interest which is essential for the Data Subject's life". Only relevant for the life-saving businesses around!

#### *5. processing is necessary for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data is disclosed;*

The phrase 'public interest', as the first UK Calcutt Report noted "means different things to different people"; in other words, the phrase has uncertain application. However this would legitimise processing by public authorities in order to exercise their legal obligations.

*6. if processing is necessary for a purpose that concerns a legitimate interest of the controller or of such a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy.*

This principle sets up a balance between two interests. Thus, if the consequences of the processing are detrimental to a particular individual, and there are no other “necessary” grounds that would take precedence, then one would expect the individual’s interests to override the controller’s interests in the continuation of the processing. One would always expect the individual’s interests to prevail if the controller acted unlawfully (e.g. did not comply with the provisions of the Act). In the absence of unambiguous consent, and given the restricted applicability of the other four cases of allowable processing, “processing for a purpose that concerns the legitimate interest of the controller” will probably be relied upon by most organisations who consistently process data for internal purposes such as customer profiling, customer profitability, etc.

### ***Bad News for Direct Marketing***

To make sure that the Data Protection Act will forever haunt marketing departments across the country, Section 10 of the Act provides that personal data may not be processed for purposes concerning direct marketing, if the data subject gives notice in writing to the controller of personal data that he opposes such processing. The controller must appropriately inform the data subject of his right to oppose, at no cost, such processing.

This section will no doubt require those businesses who rely on direct marketing, notably the banks, insurance companies, investment services providers, catalogue companies and other “mass mailers”, to conduct an exercise across all their customers to inform them of their right to object to processing for direct marketing purposes. When consent for processing is required, such consent may also be withdrawn, but it is unclear whether an objection under Section 10 may be withdrawn in the future.

### ***Customers asking to know what you know about them***

Upon request in writing, the controller of personal data must inform an individual, in writing, without excessive delay or expense, whether personal data concerning him or her is processed, and if so:-

- (i) what information is actually processed;
- (ii) where this information has been collected;
- (iii) the purpose of the processing;
- (iv) to which recipients or categories of recipients the information is disclosed; and
- (v) knowledge of the logic involved in any automatic processing of data concerning the data subject.

Most businesses will probably implement a standard form of reply to achieve compliance with these requirements. When “tell me what you know about me” requests start coming in, major difficulties will probably arise in relation to manual files and archived data. Therefore each business should conduct an exercise to identify all data sources and a method implemented to allow retrieval of information without excessive delay.

The reference to providing "knowledge of the logic" involved in automatic processing is of particular concern. Recital 41 to the EU Directive emphasises that the right to know must not adversely affect intellectual property rights including trade secrets provided that this does not result in the provision of no information whatsoever. The techniques, and also the criteria, used in automated decision making are likely to be covered by this provision.

Furthermore, individuals may request controllers to immediately rectify, block or erase personal data that has not been processed in accordance with the Act or regulations made under the Act. This could be a very powerful weapon: a business could find it difficult to refuse individuals who say "you have not complied with Section X. Now delete my data". In all probability such a request for erasure would be consequential to a request for information.

### ***Security of Processing***

The controller of personal data must implement appropriate technical and organisational measures to protect the personal data that is processed against accidental destruction or unlawful forms of processing thereby providing an appropriate level of security that gives regard to the:

- (a) technical possibilities available;
- (b) cost of implementing the security measures;
- (c) special risks that exist in the processing of personal data;
- (d) sensitivity of the personal data being processed.

Most businesses will therefore probably need to beef-up the security of the personal data they hold.

### ***Notification of Processing -or- Personal Data Representative***

The controller of personal data must notify the Data Protection Commissioner before carrying out any wholly or partially automated processing operation or set of such operations intended to serve a single purpose or several related purposes. This notification is not necessary if the controller has appointed a personal data representative and this has been notified to the Commissioner. Removal from office of a personal data representative shall also be notified to the competent authority.

The personal data representative has the function of independently ensuring that the controller of personal data processes personal data in a lawful and correct manner and in accordance with good practice and also points out any inadequacies to the controller. If the personal data representative has reason to suspect that the controller of personal data contravenes the provisions applicable for processing personal data and if rectification is not implemented as soon as practicable after being pointed out, the personal data representative must notify this situation to the Commissioner. The personal data representative can also consult the Commissioner in the event of doubt about how the rules applicable to processing of personal data should be applied. Given the obligations of a personal data representative, especially the duty to report to the Commissioner and the duty to assist data subjects, do not appear to allow an employee to be a company's personal data representative.

### ***Liability for Breach of Data Protection***

An individual may sue the controller who processes data in contravention of the Act for damages. The reference to damages is to be construed under normal rules of civil law i.e. actual

damages and not moral damages. Nevertheless, recent cases in Malta have established the right to moral damages in cases of a constitutional nature, and since data protection is a by-product of the right to privacy, there is the possibility that the Courts would interpret violations of the Data Protection Act as giving rise to liability for moral damages.

If the Data Protection Commissioner concludes that personal data is processed or may be processed in an unlawful manner, he may order rectification, and if rectification is not effected or if the matter is urgent, the Commissioner may prohibit the controller of personal data to continue processing the personal data in any manner other than to store that data, and impose an administrative fine on the controller. The extent of the fine still has to be established by regulations.

Criminal offences are committed by any person who provides untrue information to data subjects or to the Commissioner, processes personal data in contravention of certain provisions of the Act, transfers personal data to a third country in contravention of the Act or omits to notify processing to the Commissioner. The offence carries a fine not exceeding Lm10,000 or to imprisonment for six months or to both such fine and imprisonment.

Breach of the principles of processing described earlier is not a criminal offence: this sanction is reserved to breaches of processing of sensitive personal data and data relating to criminal offences. The other expression, which needs some interpretation, is "provides untrue information to data subjects". The circumstances in which information is provided to data subjects are:

- information to the data subject of his right to object against processing for direct marketing;
- information on the identity of the controller and the purposes of the processing, etc.;
- information on disclosure of data to third parties;
- information requested by the data subject on whether his data is processed;

Therefore using the data for direct marketing when the customer has shown his objection is not a criminal offence, though of course it could give rise to an administrative penalty or to a claim for damages.

### ***Conclusion***

Information is an asset that we take for granted. It is also a tool, one that is of growing importance in today's society. The Data Protection Act now addresses the concerns of how information about people is used. Personal data can give the controller a degree of power over the data subject, a power that can be abused. It is therefore important for all businesses to reassure their customers that their data is being handled properly and responsibly in accordance with the principles of data protection. This will build up the reputation of your business with a view to establishing stronger long-term customer relationships.