Malta Bankers' Association

Data Protection Commissioner

DATA PROTECTION GUIDELINES

GUIDELINES FOR THE PROMOTION OF GOOD PRACTICE

THE BANKING SECTOR

October 2008

A. Introduction

The aim of the Data Protection Act (Chapter 440 of the Laws of Malta) is to protect each individual's right to privacy with respect to the processing of personal data relating to such individuals. The Act transposed into Maltese law the provisions of the EU Data Protection Directive 95/46/EC. Furthermore, under the provisions of the Act, Legal Notice 16 of 2003 transposed the EU Privacy and Electronic Communications Directive 2002/58/EC.

In line with their obligations under the Act, banks invest in the latest technologies and training of all staff to ensure that the confidentiality and integrity aspect of customer information and data are assured.

The Act came into force on 15 July 2003. However, the provisions of certain Articles (7 to 9 and 12 to 17) only apply from 24 October 2007 onwards where processing operations of personal data held in **manual** filing systems had already been initiated prior to 15 July 2003.

Processing of personal data in the electronic communications sector is regulated by Legal Notice 16 and Legal Notice 19 of 2003 which transposed the provisions of Directive 2002/58/EC into Maltese law.

These Guidelines have been developed after a consultation process with the Data Protection Commissioner who, in terms of Article 40(g) of the Act, has the function to encourage the drawing up of suitable codes of conduct by the various sectors and who, in terms of this Article, ascertained that the provisions of these Guidelines are in compliance with the Act.

The purpose of these Guidelines is not to provide a detailed and comprehensive coverage of the whole Act. Rather, these Guidelines are intended to focus only on those areas which are most relevant to the banking sector. The Guidelines also seek to address those sections of the Act which may not be entirely clear, or which could lend themselves to differing interpretations, in order that a common understanding is arrived at and a consistent interpretation is applied across the banking sector.

The Guidelines will be further developed over time, as practical issues and problems arise, and the banks' coordinated response to such issues is agreed and documented in the Guidelines.

B. An Overview of the Act

1. Guiding Principles

The guiding principles on which the Act is based are stated in Article 7 ('Requirements for processing'), and these are worth recalling at the outset as any reading or interpretation of other sections must be consistent with these principles.

Article 7 requires a controller (the person who determines the purposes and means of processing of personal data) to ensure that:

a. personal data is processed fairly and lawfully;
b. personal data is always processed in accordance with good practice;
c. personal data is only collected for specific, explicitly stated and legitimate purposes;
d. personal data is not processed for any purpose that is incompatible with that for which the information is collected;
e. personal data that is processed is adequate and relevant in relation to the purposes of the processing;

f. no more personal data is processed than is necessary having regard to the purposes of the processing;

g. personal data that is processed is correct and, if necessary, up to date;

h. all reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which they are processed;

i. personal data is not kept for a period longer than is necessary, having regard to the purposes for which they are processed.

The link to the purpose specified at the point of collection of personal data 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.

2. When is Processing of Personal Data Permitted?

Apart from the purpose detailed in Article 7 of the Act, processing must also satisfy the criteria under Article 9. This Article lists six scenarios under which personal data may be lawfully processed:

a. *If the data subject has unambiguously given his consent.*

By definition, consent must be freely given, specific and informed. Although there is no legal obligation that consent should be in writing, it is good practice if consent is confirmed in writing. The individual may revoke his consent at any time for compelling legitimate grounds. If the individual has not given his consent to the processing, the processing is only allowed if it falls under one of the following five headings.

b. *If processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.*

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

c. *If processing is necessary for compliance with a legal obligation to which the controller is subject.*

This covers processing due to statutory duties imposed by law on controllers, e.g. reporting to the tax authorities, or reporting of suspicious transactions under the Prevention of Money Laundering and Funding of Terrorism Regulations.

d. *If processing is necessary 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'. This is the definition given by the Data Protection Commissioner.

e. *If 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.*

This allows processing of personal data by public authorities in order to exercise their functions and meet their legal obligations.
This article may also be utilised when processing of personal data is necessary for the performance of an activity that is carried out in

the public interest. The notion of public interest is developed mainly through case law.

f. *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.

The Necessity Factor

The use of the word 'necessary' in Article 9 (b)–(f) should not be overlooked. This word

implies that under these provisions, only that processing without which the intended purpose will be rendered impossible or impractical is allowed.

3. Direct Marketing

The processing of personal data for purposes concerning direct marketing is regulated by Article 10 of the Act and by Regulation 10 of Legal Notice 16 of 2003. These legislative provisions, as they apply to communications for direct marketing purposes by electronic mail or by conventional mail, are explained in Section C, paragraph 2, of the Guidelines.

4. Processing of Sensitive Personal Data

Articles 12 to 16 of the Act deal with the processing of 'sensitive personal data', which is given particular treatment.

‘Sensitive personal data’ is defined as ‘personal data that reveals race or ethnic origin, political opinions, religions or philosophical beliefs, membership of a trade union, health or sex life.’

Except in certain clearly defined cases, the Act only permits the processing of sensitive personal data if the data subject:

a. has given his explicit consent to processing; or
b. has made the data public.

The exceptions which are relevant to the banking sector are listed in Article 13. This permits the processing of sensitive personal data if appropriate safeguards are adopted, and the processing is necessary in order that:

a. the controller will be able to comply with his duties or exercise his rights under any law regulating the conditions of employment; or
b. the vital interests of the data subject or of some other person will be able to be protected and the data subject is physically or legally incapable of giving his consent; or
c. legal claims will be able to be established, exercised or defended.

5. Processing concerning Legal Offences

Article 17 of the Act restricts the processing of personal data concerning legal offences. Data relating to offences, criminal convictions or security measures may only be processed 'under the control of a public authority'.

Having said that, the Minister responsible for data protection may issue Regulations authorising any person to process such data, subject to suitable specific safeguards; but still, a complete register of criminal convictions may only be kept 'under the control of a public authority'. To date no such Regulations have been issued.

6. Data Subjects' Right of Access to Information

Upon request, a controller of personal data is obliged to provide a data subject, without excessive delay and without expense, with written information as to whether personal data concerning the data subject is

processed. If so, the controller must advise the data subject in writing and in an intelligible form about:

- what information is actually processed;
- where this information has been collected from;
- the purpose of the processing;
- to which recipients the information is disclosed;
- knowledge of the logic involved in any automatic processing of data concerning the data subject.

7. Rectification

Data subjects may request controllers to rectify, block or erase personal data that has not been processed in accordance with the Act, in particular because of the incomplete or inaccurate nature of the data.

On good cause being shown, the controller shall immediately rectify, block or erase the data accordingly, and notify any third parties to whom data had been disclosed about the measures undertaken.

8. Transfer of Data to Third Countries

Such transfers are regulated by Articles 27 and 28 of the Act, and by Legal Notice 155 of 2003 – 'Third Country (Data Protection Act) Regulations, 2003'.

A transfer of personal data to another country constitutes processing and as such must be notified to the Commissioner in the same way as other processing operations. No restrictions or other formalities apply in relation to transfer of personal data to:

i) EU Member States;
ii) Member States of the EEA; and
iii) Third countries (i.e. countries that are not Member States of the European Union) which are from time to time recognised by the EU Commission to have an adequate level of protection.

The transfer of personal data to a third country that does not ensure an adequate level of protection is prohibited, (unless the data subject has given his unambiguous consent or in certain other specified cases), and data controllers must

therefore request the prior approval of the Commissioner. In his consideration, the Commissioner will ensure that the procedures adopted are those standard contractual clauses established by the EU Commission.

9. General

The above overview touches on those provisions of the Data Protection Act which are most relevant in the context of the banker-customer relationship. Further comment is made in section C, which follows, on certain specific issues which warrant further elaboration or clarification.

C. Comments on Specific Issues which are relevant to the Banker/Customer Relationship.

1. Consent

1.1 Processing of personal data by banks is normally performed after obtaining the unambiguous consent of the data subject, or when the processing of the customer's data is a necessary element in providing the service requested by the customer himself.

1.2 Data which is not required for providing the service requested by the customer should only be collected with the customer's consent. Moreover, when making an application, an applicant should be in a position to reasonably ascertain whether he is providing information which is not strictly required for the delivery of the service requested. Indeed, the Act requires a data controller to inform a data subject from whom personal data is being collected "whether the reply to any questions made to the data subject is obligatory or voluntary", as well as "the possible consequences of a failure to reply".

1.3 There are also cases, however, where notwithstanding that consent has not been sought, and that processing is not necessary for providing the particular banking service, it is in the banks' legitimate interest to process personal data. This is allowed under the Act unless there is an overriding interest of the customer.

Lending, in particular, is one of the banks' major business activities, and "Loans and Advances to Customers" normally account for a large proportion (+50%) of their total assets. Such business carries significant potential credit risks which banks must manage with great caution and prudence in the interests of their shareholders, customers, staff and the financial services industry in general.

For this reason, banks consider it vital and certainly in their legitimate interest to maintain relevant information to alert their lending officers to the risks of making new or further advances to certain individuals who, on the basis of past experience, clearly do not qualify for such new or additional lending.

1.4 The "Know Your Customer" principle is particularly relevant to bank business, and banks must seek to have maximum knowledge of a prospective customer's affairs, including details of his background, means, etc. This is also necessary for banks to comply with the due diligence procedures which are called for under the anti-money laundering and funding of terrorism legislation. It is legitimate for banks to process such data internally, without notifying customers or seeking their consent, when such processing is carried out for the purpose of producing customer profiling/segmentation/profitability analyses, thereby enabling the bank to render a better service to their customers through a more efficient and effective targeted approach.

2. Direct marketing

2.1 Communications for direct marketing purposes by means of an automatic calling machine, a facsimile machine or electronic mail are regulated by Legal Notice 16 of 2003 as amended by Legal Notice 153 of 2003, Legal Notice 522 of 2004 and Legal Notice 109 of 2005, and are hereunder referred to as 'communications by electronic means'. All other types of communications for direct marketing purposes are referred to as 'conventional mail'.

2.2 Conventional Mail:

The processing of legitimately collected personal data for direct marketing purposes is allowed as long as the data subject does not give notice to the controller that he opposes it.

The controller is duty bound to appropriately inform the data subject of his right to oppose, at no cost, the processing for direct marketing purposes. In practice, this is normally done at the beginning of a relationship.

If no objection has been/ is received, banks may continue to process these customers' data for direct marketing purposes by conventional mail.

2.3 Communications by Electronic Means:

Regulation 10(1) of Legal Notice 16 of 2003 prohibits the use of an automatic calling machine, or a facsimile machine, or electronic mail to make an unsolicited communication to a subscriber (whether a natural person or a legal person) for the purpose of direct marketing, **unless that subscriber has given his prior explicit consent in writing to the receipt of such a communication**.

However, Regulation 10(2) of the Legal Notice allows some leeway in this regard, in that where a customer's contact details for electronic mail have been obtained by a bank '…in relation to the sale of a product or service', that bank may use such contact details '…for direct marketing of its own similar products or services.' But this leeway comes with a Proviso: 'That customers shall be given the opportunity to object … to such use of electronic contact details when they are collected and on the occasion of each

message where the customer has not initially refused such use'.

2.4 Stationery issued by banks, such as bank account statements, ATM receipts, transaction vouchers etc. may contain general additional information about the services offered by the bank. This information is not equivalent to unsolicited advertising and the customer's right to opt-out does not apply in relation to this information.

3. Information to data subject

3.1 CCTV:

Video surveillance constitutes processing of personal data. Persons within the monitored area must be aware that they are being monitored. For this purpose banks should affix appropriate signs, which are clearly visible, on the façade of their premises. The signs should clearly state the purpose of processing.

Normally, CCTV recordings within a bank are used for security purposes. It is not excluded, however, that available CCTV recordings could be used by a bank for the

purpose of an internal investigation involving a member(s) of its staff provided, however, that the staff concerned had been aware that they could have been recorded on the bank's monitoring system.

3.2 Telephone Recordings:

Recordings of telephone conversations constitute processing of personal data. Callers and staff should therefore be advised beforehand if such recording is being carried out.

3.3 Data Collected from other sources:

It is normal for banks, in the course of their business, to require references from third parties on individuals who may be existing or prospective account holders, borrowers, guarantors, etc. Such references are collected from third parties, including Credit Reference Agencies, other banks, other existing customers and professional persons.

In their capacity as employers, banks may also need to carry out background checks on prospective employees.

Whenever such information is sourced by a bank from a third party, the bank must inform the individual, on applying for a particular facility or the opening of an account, or on applying for a post with the bank, that such information will be processed.

Where it is the data subject himself who, upon request, provides the bank with the name of the third party from whom the reference is being sought, this constitutes implied consent. Also, the data subject is deemed to be appropriately informed about the collection of data about him from the third parties indicated by him.

3.4 Decisions based on automated processing:

This applies in particular to credit scoring. Where the outcome of such scoring results in a request for credit facilities being declined, the applicant is entitled to:

i) Request that the decision be reconsidered other than in manner based solely on automated processing;

ii) Obtain information from the bank about what has controlled the automated processing that resulted in the negative decision.

The bank, however, will not indicate the specific criteria which were the main contributory factors leading to the decision to decline the application.

Neither do any specific technical details or trade secrets need to be divulged.

4. Right of access

4.1 Article 21 of the Act requires banks to provide to the data subject "*written information in an intelligible form"* about the processing of personal data concerning the data subject. This article therefore does not entitle customers to gain physical access to the banks' files for viewing or perusal or to obtain a copy of the relevant file.

4.2 Due to the nature of the banks' business, it is important to distinguish between the provision of information as required under Article 21 of the Act and providing information as part of the bank's services to its clients e.g. bank statements. The right of access may not be invoked

by clients to try and obtain these services without incurring any charges.

4.3 In response to such requests, banks may not be aware of particular information that is stored in files not pertaining directly to the person making the enquiry e.g. deceased customers' files containing details of the heirs, corporate client files containing details of individual shareholders and directors, etc… In such cases banks are not to be expected to include such information in their response.

4.4 Any personal data relating to third parties and contained in the file of a customer making a request may not be included in a reply to an access request. Provided that such third party information may be disclosed to the person making the request after the bank has obtained the consent of such third party.

However in the case of a joint account, all parties to the account may have access to information relating to transactions passed over that account, notwithstanding that some or all of the transactions may have been originated by another joint account holder.

4.5 Article 21(2)(v) requires banks responding to such requests to provide information about 'knowledge of the logic involved in any automatic processing of data concerning the data subject'.

In this regard, no specific technical details or trade secrets would need to be divulged by the banks, though the logical sequence of such processing would need to be explained.

4.6 Banks are not in a position to accede to requests by individuals to view CCTV recordings. Such recordings will only be made available to the Police, upon formal request, to assist them in any investigations which they may be carrying out.