



Data Protection Commissioner

DATA PROTECTION GUIDELINES

GUIDELINES FOR THE PROMOTION OF GOOD PRACTICE

FUNDS SECTOR

These guidelines have been developed in consultation with the Malta Financial Services Authority, the Malta Funds Industry Association and the Institute of Financial Services Practitioners.

This consultation process is in line with the obligations of the Data Protection Commissioner who, in terms of article 40(g) of the Data Protection Act (“the Act”), has the function “*to encourage the drawing up of suitable codes of conduct by the various sectors affected by the provisions of this Act.*”

Unless otherwise provided for throughout this document, these guidelines are applicable in the case where a locally domiciled Collective Investment Scheme licensed under the Investment Services Act, acting either directly or through an agent or intermediary, is the ultimate collector of the data.

The purpose of these Guidelines is not to provide a detailed coverage of the Act or replace the provisions thereof. Rather, they are intended to provide a platform for the promotion of good practice in the funds business and assist data controllers in the practical application of data protection principles in the course of their business.

These guidelines are primarily aimed at protecting the privacy of investors in collective investment schemes in relation to the processing of personal information.

Drawn up in consultation with:

MFSA
MALTA FINANCIAL SERVICES AUTHORITY

October 2009

Contents

1	Terminology	4
2	Application of the Act	5
3	Notification Obligations	7
4	Consent	9
4.1	Collection of data relating to data subjects	10
4.2	Surrender/ Redemption Stage	10
4.3	Appointing an agent/intermediary	10
4.4	Consent form.....	11
4.4.1	Informed consent	11
4.4.2	Freely given consent	12
4.4.3	Specific consent	12
4.5	Right to revoke consent	12
5	Right to Information	13
5.1	Multi-layered notices	13
5.1.1	The short notice.....	13
5.1.2	The condensed notice.....	13
5.1.3	The full notice	14
6	Right of Access.....	14
6.1	Cases where the right of access does not apply	15
7	Other obligations	16
8	Transfer of Personal Data within a Group.....	17
	Annex 1: Notification Form.....	18

1 Terminology

The definition of the following terms will assist in the better understanding of these guidelines.

- “CIS” means a Collective Investment Scheme licensed under the Investment Services Act;
- “data controller” or “controller” refers to the person who alone or jointly determines the means and purposes of the processing of personal data; in the context of collective investment schemes, the data controller would be one of the following:
 - (a) the Scheme itself as represented by its board of directors in the case where it is set up as an investment company under the Companies Act;
 - (b) the Scheme itself as represented by its General Partners in the case where it is set up as limited partnership under the Companies Act;
 - (c) the Scheme itself as represented by its Trustee in the case where it is set up as a unit trust under the Trusts and Trustees Act;
 - (d) the Scheme itself as represented by the Management Company in the case where it is set up as common contractual fund under the Civil Code.

An investment intermediary investing client’s money in its own name in a collective investment scheme is also considered to be a data controller. The transfer of personal data between the investment intermediary and the CIS in such a situation is equivalent to a transfer of data between different data controllers.

In other words, licensed intermediaries investing clients' money in their own name would be independent controllers of their client information.

- “data subject” refers to a natural person to whom the personal data relates; in the context of funds, this refers to the unit-holder;
- “Fund Administrator” refers to a person who is in possession of a recognition certificate issued by the Malta Financial Services Authority to act as an administrator of a CIS, in or from Malta, in terms of article 9A of the Investment Services Act.
- ‘ISA’ refers to the Investment Services Act (Cap 370);
- “personal data” means any information relating to an identified or identifiable natural person; accordingly the provisions of the Act do not apply to data relating to institutional investors, investment vehicles or entities so long as no personal data relating to an individual is involved;
- “Scheme” means a Collective Investment Scheme licensed under the Investment Services Act;
- “the Act” refers to the Data Protection Act (Cap 440).

2 Application of the Act

These Guidelines refer to the control and processing of personal data which, of its own nature, is inherent to the funds business. The Guidelines are not intended to cover the data of a general nature which is applicable in a different context such as data collected for employment purposes or for direct marketing

purposes, although this type of data may still fall within the scope of the Act.

The terms ‘personal data’ in an investment fund context do not extend to data related to a juridical person such as an institutional or corporate investor. The Act only extends to relating to an identified or identifiable natural person¹.

The Act applies to **processing** of personal data whether this is held on computer or intended to form part of a filing system and is carried out either by automated or physical means.² The Act applies to the processing of information by an **establishment** of a data controller in Malta, and to the processing by means of equipment situated in Malta controlled by a person established in a country other than a European Union Member State or within the European Economic Area.³

The processing operations which are relevant to the funds sector are mainly the following:

- Promoting the fund to new clients
- KYC procedures (Anti-Money Laundering proceedings)
- Compilation of the application form
- Preparation of contract notes
- Communicating fund or investment performance details
- Filling of redemption forms
- Effecting redemptions

¹ The Act also defines “identifiable person” as being 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.

² Article 3 of the Act

³ Article 4 of the Act

2.1. Data Process Outsourcing:

Unless the circumstances suggest the contrary, the transfer of data between the CIS and the investment manager and/or fund administrator in relation to the provision of management and/or administrative services to the CIS would normally be considered as equivalent to the transfer of data between the data controller (the CIS) and the data processor (the investment manager/fund administrator). The investment manager and the fund administrator are normally contracted by the CIS and should therefore be considered as processors.

Where data processing is undertaken by a data processor on behalf of the data controller, such processing shall be regulated by a contractual agreement⁴. The CIS shall further ensure that the relevant contract requires the data processor to take the relevant security measures relating to the processing of the data.⁵

3 Notification Obligations

Data controllers have an obligation to notify the Data Protection Commissioner of any processing operations as aforesaid⁶. In the context of these Guidelines, the primary responsibility to effect such notifications rests with the CIS. Although in practice, the Scheme may be assisted by its Service Providers (for example the investment manager or fund administrator) in the Notification Process, it is the Scheme and not its third party contractors who are responsible for the notification obligations relating to the CIS.

⁴ Article 25 of the Act

⁵ Article 26 of the Act

⁶ Article 29 of the Act

The Notification shall be submitted by the data controller acting through its representative⁷ and it is made through the Notification Form made available by the Office of the Data Protection Commissioner. A copy of the aforementioned Notification Form is being annexed to these Guidelines and marked Annex 1⁸.

In the case of a Scheme that is established in the form of a multi-fund company incorporating a number of sub-funds, the notification should specify any differences in the data processes or other reportable information that may exist between the various sub-funds.⁹

The Data Protection Commissioner must also be informed of any new, discontinued or amended processing operations. Notification is to be made on the appropriate form.

Notification is not an annual requirement but any addition, discontinuation or amendment from the original notification form has to be notified as soon as it occurs, also on the appropriate form.

An annual fee of €23.29 is due by data controllers who are obliged to notify their processing operations¹⁰.

⁷ Reference is to be made to the definition of “Data Controller” reported in Section 1 of these Guidelines.

⁸ This form can also be downloaded from the website of the Office of the Data Protection Commissioner from the following link: <http://www.dataprotection.gov.mt/dbfile.aspx/Notification%20Form%20Final%20Version.pdf>. Also available on the said website is a “Guide to completing the Notification Form”.

⁹ Under the Companies Act (Investment Companies with Variable Share Capital) Regulations (LN241 Of 2006) a "sub-fund" means the distinct class or classes of shares constituting that sub-fund in a multi fund company to which are allocated assets and liabilities distinct from other assets and liabilities allocated to other sub-funds in the same company.

¹⁰ L.N. 154 of 2003 - Notification and Fees (Data Protection Act) Regulations, 2003 as amended by L.N. 162 of 2004

Independent financial intermediaries who invest clients money in CISs (among other instruments), have their own independent obligations under the Data Protection Act, as controllers of data related to their clients.

4 Consent

Article 9 of the Act requires the data controller to obtain the data subject to give consent to the processing of his/her personal data in certain situations. This Article also lists those situations in which the data subject may not be required to give consent.

A distinction exists between personal data, the processing of which requires the unambiguous consent of the data subject¹¹, and sensitive personal data, which requires explicit consent¹². In either case consent must be freely given, specific and informed¹³.

CISs may therefore need to seek consent from the investor in certain circumstances and in the appropriate format. Every CIS should therefore carefully consider whether it would need to obtain the consent of the investor in the course of its dealings with the investor, such as at the stage of:

- ▶ Subscription (Application Form)
- ▶ Surrender or Redemption of Units
- ▶ Changing between different sub-funds of the Scheme.

¹¹ Article 9(a) of the Act

¹² Article 12(2)(a) of the Act

¹³ Reference must be made to the definition of ‘consent’ reported in Article 2 of the Act

4.1 Collection of data relating to data subjects

Where an agent applies for units in a fund on behalf of an investor, personal data is not collected directly from the data subject himself. The agent in this case is deemed to be acting on behalf of the data subject and is therefore deemed to have obtained the consent thereof for the purpose of acquiring units in the fund. Information about a data subject may not be processed where the latter opposes such processing.

In cases involving the processing of sensitive personal data, the agent should be in a position to obtain the explicit consent of the data subject. In such contracts it is the responsibility of the agent to ensure that such explicit consent has been given by every individual acting as data subject under the said contract.

4.2 Surrender/ Redemption Stage

A redemption form is completed by the collection of the data required for the redemption of units to be processed. During the surrender stage the data subject is consenting to the processing of additional personal data (if any) that is relevant to the redemption of units such as a declaration by the data subject that he/she is the lawful and beneficial owner of the units or a confirmation that the units are free and unencumbered.

Where the data controller must establish, exercise or defend legal claims in relation to the surrender which requires the processing of sensitive personal data, the explicit consent is not required¹⁴.

4.3 Appointing an agent/intermediary

Agents are chosen by the investors to act on their behalf and do everything necessary in their best interest so as to comply with their request for a subscription of units in a specific fund.

¹⁴ Article 13(c) of the Act

Since the agent is appointed by the data subject, the latter signifies his/her consent to the agent to process personal data for the purpose of acquiring units in a fund in the name and on behalf of the data subject. If the personal data so required is sensitive personal data, the consent shall be explicit.

In the above-mentioned cases, the requirement of consent in terms of the Act is deemed to be satisfied and the agent may process the personal data to the extent that this is necessary to provide the data subject with the service requested by same.

4.4 Consent form

Although there is no obligation at law for consent to be in writing, it is good practice, for consent to be obtained on a form signed by the data subject. Such form should be drafted in a way so as to enable the controller to obtain the informed, freely given and specific consent of the data subject.

4.4.1 Informed consent

For consent to be valid, the data subject is to be informed in a concise and clear manner on the purpose for processing. Such information will distinguish between essential information and possible “further” information. Essential information needs to be provided at all data collection stages. In determining what essential information is, the controller should provide the data subject with sufficient information for the latter to be able to give his informed consent at that point in time. “Further” information must be provided where it is necessary to guarantee fair processing having regard to the specific circumstances in which the data are collected.

4.4.2 Freely given consent

Where the controller wishes to seek consent for processing of data which is not strictly necessary for the performance of the contract, the consent form must be drawn up in a manner which distinguishes between the consent given for ‘mandatory processing’ and the consent given for other processing. The data subject will in this way consent for the ‘mandatory processing’ without prejudicing the right not to consent to other processing.

4.4.3 Specific consent

Since consent should be obtained for specific purposes, the terminology used in the consent form should not be in general terms but has to be specific having regard to the processing purpose.

4.5 Right to revoke consent

The data subject may, on compelling legitimate grounds, revoke the consent previously given with regards to the processing of personal data¹⁵. Revocation of consent should only be permissible in relation to consent given for processing of data which is not inherent to the purchase or redemption of units in a fund. Therefore, the term ‘compelling legitimate grounds’ should not be interpreted in a way so as to legitimise any action which is not acceptable in terms of the fund’s prospectus or in any case of a fraudulent intention of the unit holder as data subject.

Thus the data subject may not revoke his/her consent in any of the following cases where:

- ▶ data is being processed for the purpose of preventing fraud;

¹⁵ Article 11 of the Act

- ▶ the personal data in question is necessary to satisfy the instructions given in origin to the agent;
- ▶ the processing of personal data is necessary for the controller to defend himself pending a dispute between the controller and the data subject.

- ▶ the recipient of the data;
- ▶ whether replies to any questions are obligatory or voluntary, as well the possible consequences of failure to reply;
- ▶ the possibility of transfer of the data to third parties¹⁷; and
- ▶ the right to access, the right to rectify and where applicable the right to erase the data concerning him/her.

5 Right to Information

Where information needs to be provided to a data subject, such information shall be clear and understandable¹⁶. Controllers are encouraged to make this information available on-line, in a hard copy and by phone. It is good practice to provide information in a multi-layered structure.

5.1 Multi-layered notices

5.1.1 The short notice

Data subjects are to be provided at least with the core information namely, the identity of the data controller, the purposes of processing and any additional information which, in the particular circumstances of the case, must be provided to ensure fair processing. This notice should then indicate access to additional information.

5.1.2 The condensed notice

Data subjects must at all times be able to access the following information:

- ▶ the identity and habitual residence or principal place of business of the data controller;
- ▶ the purpose of processing of data;

¹⁶ Articles 19 and 20 of the Act

Additionally a point of contact must be given for questions and information on redress mechanisms.

5.1.3 The full notice

This layer must provide all information possible on the processing operations by the controller. This is usually captured in a privacy policy.

6 Right of Access

In the absence of exceptional circumstances, the data subject has the right to access his/her personal data¹⁸.

Upon receipt of a written request by the data subject, the data controller is obliged to confirm whether any personal data concerning such data subject is being processed. The request must be signed by the data subject. The reply must be given:

- ▶ in writing;
- ▶ without excessive delay;
- ▶ without expense; and
- ▶ in an intelligible form.

¹⁷ For example data transferred from an intermediary to the Scheme, or between a Scheme and a third party administrator.

¹⁸ Article 21 of the Act

Where data is so processed, the data controller must provide the data subject with the following information:

- ▶ the actual information about the data subject which is being processed;
- ▶ the source of the information;
- ▶ the purpose of the processing;
- ▶ the recipients or categories of recipients to whom this data is being disclosed; and
- ▶ knowledge of the logic involved in any automatic processing of data relating to the data subject.

This means that, as long as the above information is provided, the right of access does not require the data controller to give the data subject physical access to the personal data or to provide him/her with a copy of the data. However the data controller may opt to give physical access or to provide a copy of all data relating to the particular data subject.

In providing the right of access the controller may not reveal personal data relating to third parties, and the rights of the data subject for access have to be balanced with the fundamental rights and freedoms of others.

6.1 Cases where the right of access does not apply

The right of access shall not be allowed in circumstances where such right, if exercised, would be prejudicial to protection of the data subject or the rights and freedoms of others¹⁹.

However this exemption from the right of access shall not apply in relation to all personal data, but only to such data, the provision of which, would result to be prejudicial to the controller; in this case the controller has to be able to prove such

¹⁹ Article 23(1)(g) of the Act

prejudice. Actual prejudice has to be determined on a case-by-case basis.

Upon cessation of the ground for prejudice the right of access must be re-instated by the data controller immediately.

7 Other obligations

The Act contains other obligations that a CIS or its officers may need to comply with, such as:

- ▶ certain types of information are considered sensitive and may be subject to additional conditions as described in Part IV of the Act – for example, the processing of identity card numbers in the absence of consent may only be made under certain conditions;²⁰
- ▶ at the request of the data subject, the data controller shall rectify personal data that has not been processed according to the Act;²¹
- ▶ the data controller shall notify the Data Protection Commissioner on the appointment or removal of a personal data representative;²²
- ▶ the personal data representative shall independently monitor the processing operations as outlined in the Act;²³ maintain a register of notifiable processes;²⁴
- ▶ assist the data subject to exercise his rights under the Act.²⁵

²⁰ Article 18 of the Act

²¹ Article 22 of the Act

²² Article 30 of the Act

²³ Article 31 of the Act

²⁴ Article 32 of the Act

²⁵ Article 33 of the Act

8 Transfer of Personal Data within a Group

Companies within a group have a separate juridical personality and are separately responsible for the processing of personal data. Therefore a transfer of personal data between members of the same group is equivalent to a transfer of data between different data controllers.

In cases where the transfer does not involve sensitive personal data, the said transfer is legitimate when the data subject has given his unambiguous consent²⁶ or when the processing is necessary for the performance of the contract between the data subject and the controller²⁷ or when the processing is necessary for a purpose that concerns a legitimate interest of the controller or of such third party to whom personal data is provided²⁸.

Where personal data is transferred to a third country (Non EU/EEA) that is not recognised by the EU Commission as ensuring an adequate level of data protection, such transfer shall only occur subject to appropriate safeguards being implemented and further to the authorisation of the Data Protection Commissioner²⁹.

Further information:

Further information on the completion of the Notification Form may be found in the **Guide to completing the Notification Form** which is available under the Notifications section on the Data Protection Commission's website: www.dataprotection.gov.mt


²⁶ Article 9(a) of the Act

²⁷ Article 9(b) of the Act

²⁸ Article 9(f) of the Act

²⁹ Articles 27 and 28 of the Act

Annex 1: Notification Form

<h1>Notification Form</h1>	 Office of the Data Protection Commissioner 2, Airways House High Street, Sliema SLM 16 Malta Tel: (+356) 2328 7100 Fax: (+356) 2328 7198 E-Mail: commissioner.dataprotection@gov.mt Website: www.dataprotection.gov.mt
<ul style="list-style-type: none">Processes for first notification by Data Controller.Date when processes first commenced <input type="text"/>Please complete this Form in BLOCK CAPITALS.	
1. Details of Data Controller	
1.1 Name of Organisation:	<input type="text"/>
Trading Name(s):	<input type="text"/>
Head of Organisation:	<input type="text"/>
Business Address:	<input type="text"/>
Telephone Number:	<input type="text"/>
Fax Number:	<input type="text"/>
Website address:	<input type="text"/>
E-Mail Address:	<input type="text"/>
VAT REG. Number: (if applicable)	<input type="text"/>
Company REG. Number/ ID Card Number:	<input type="text"/>
1.2 Contact Person within organisation (if different from above)	
Name:	<input type="text"/>
Address:	<input type="text"/>
Telephone Number:	<input type="text"/>
Fax Number:	<input type="text"/>
E-Mail Address:	<input type="text"/>

2. Details of Personal Data Representatives (if the Data Controller opted to appoint a Personal Data Representative)

Name:

Address:

Telephone Number: Fax Number:

E-Mail Address:

Data Controllers are advised that Regulations on the qualifications of PDRs are to be issued in the near future. However the PDR can still be appointed now.

3. Type of Organisation (Tick where appropriate)

Government Department	<input type="checkbox"/>	Public Corporation or Authority	<input type="checkbox"/>
Health	<input type="checkbox"/>	Self-employed with no employees	<input type="checkbox"/>
Co-Operative	<input type="checkbox"/>	Sole Trader	<input type="checkbox"/>
Education	<input type="checkbox"/>	Professional Office	<input type="checkbox"/>
Financial Services:		Foundation/Association	<input type="checkbox"/>
Bank	<input type="checkbox"/>	Civil Partnerships	<input type="checkbox"/>
Insurance	<input type="checkbox"/>	Company	<input type="checkbox"/>
Credit Agencies	<input type="checkbox"/>	Others	<input type="checkbox"/>
Other Financial services	<input type="checkbox"/>	Specify: <input type="text"/>	

4. Nature of Business

5. Purposes of processing and categories of data relating to them
(Use additional sheets if necessary)

5.1 Processing Operations and a brief description of purpose

5.2 Categories of data subjects about whom processing is performed.
Tick as appropriate (you can tick more than one category)

Employees & staff members (including directors)	<input type="checkbox"/>	Correspondents/Enquirers	<input type="checkbox"/>
Customers/clients	<input type="checkbox"/>	Suppliers	<input type="checkbox"/>
Shareholders	<input type="checkbox"/>	Students	<input type="checkbox"/>
Social Assistance Beneficiaries/Individuals	<input type="checkbox"/>	Patients	<input type="checkbox"/>
Members/Supporters	<input type="checkbox"/>	Relatives/Guardians	<input type="checkbox"/>
Others – Specify:	<input type="text"/>		

5.3 Categories of data relating to the data subject (Tick where appropriate)

Personal details which identify the data subject	<input type="checkbox"/>
Business process specific details	<input type="checkbox"/>
HR And Employment Details (including qualifications, payroll)	<input type="checkbox"/>
Financial Details	<input type="checkbox"/>
Family/Lifestyle/Social Circumstances	<input type="checkbox"/>

5.3 Cont.

Statistics/ Research Details

Others

Brief General Description:

5.4 Sensitive Personal Data *(Tick where appropriate)*

Racial & Ethnic Origin

Political Opinions

Religious or Philosophical Beliefs

Trade Union membership

Health

Sex Life

6. Recipients to whom Personal Data may be disclosed:

(Tick where appropriate)

Data Subjects themselves

Relatives/Guardians

Employees within the Organisation

Other organisations processing data on behalf of the Data Controller

Government/Regulatory Authorities

Other Third Parties

Specify:

7. Transfer of Personal Data Abroad

(Tick where appropriate)

No transfer of data is made

Data is transferred to EU Member States

Data is transferred to other third countries

Specify:

8. Security measures relating to processing

(Tick where appropriate)

To ensure an adequate level of security, indicate which measures have been implemented to protect the personal data against unlawful forms of processing:

Do all individuals who handle personal data have the necessary data protection awareness and training? Yes No

Do you have a record of persons who access the system? Yes No

Does your system include:

Logins and passwords Yes No

Access rights/privileges Yes No

Audit trails Yes No

Other measures:

Do you have physical security safeguards?

Locking of offices Yes No

Locking of file cabinets Yes No

Other measures:

9. Privacy Policy

Do you have a clearly documented statement of Data Protection Policy? Yes No

1. Providing untrue information is an offence against the Data Protection Act and attracts heavy penalties.
2. Subject to paragraph 4, notifications are not to be renewed annually but the annual fee is to be renewed to this Office by not later than 14 July of each year.
3. Any further processing operation or any other amendment to the original notification form should be communicated to this Office immediately, by amending the appropriate section(s).
4. The information provided in this form will be solely used by the Data Protection Commissioner in accordance with the Data Protection Act. Sections 1 to 7 comprise the Public Register, which according to law is held by this Office and may be viewed by members of the public at any time. For further information, you may wish to refer to our Privacy Policy which can be found on our website.

Notification Fee

The annual notification fee of Lm 10 (€ 23.29) is due by 14 July.

Fee enclosed

Exemption from the notification fee

I declare to be exempt from the payment of the annual fee being:

a self-employed with no employees; or

I declare to qualify, under sub-article (1) of article 12 of the Income Tax Act, for an exemption from the notification fee being:-

a philanthropic institution or another similar organisation which qualifies under paragraph (e) of the said sub-article; or

a *bona fide* band club which qualifies under paragraph (n) of the said sub-article; or

a *bona fide* sports club or other similar institution which qualifies under paragraph (c) of the said sub-article; or

a registered trade union; or

a political party or club adhering to political parties.

Name in Blocks:

Organisation
Rubber Stamp:

Signature:

Date:

For Office Use Only

Received by: *Date:*

Receipt No: *Reference No:*