DATA PROTECTION POLICY

1. Principles and Policy

Future Focus recognizes and upholds the importance of the correct and lawful treatment of personal data.

The objectives of this Data Protection Policy and the Data Protection Act (Malta) are:

i. To coordinate the information security and data handling procedures;
ii. To promote confidence in our information security and data handling procedures;
iii. To comply with the Data Protection Act (Malta) 1998; and
iv. To provide a benchmark for employees on information security, confidentiality and data protection issues.

Objectives will be achieved by:

i. Implementing appropriate information handling policies and procedures for employees to follow and refer to; and
ii. Regular monitoring of the effectiveness of information handling policies and procedures to make amendments and additions as necessary from time to time.

2. Defining terms

For the purposes of this Data Protection Policy Malta, the following terms shall have the following meanings:

i. ***"data"*** means information stored or processed by a computer and information recorded as part of a relevant filing system (which includes paper-based filing systems, card indexes and other non electronic collections of data which are

structured either by reference to individuals or so that information about an individual is easily accessible);

ii. ***"personal data"*** means data about a living person who can be identified by that data;

iii. ***"data subject"*** means a person who is the subject of personal data; and

iv. ***"processing***" means obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, disclosing, aligning, combining, blocking, erasing or destroying data; and

v. ***"Sensitive personal data"*** means personal data relating to physical or mental health, religious or philosophical beliefs, and membership of a Trade Union, political opinions, race or ethnic origin, information about sex life, criminal convictions or allegations of criminal conduct.

3. The Nine Data Protection Principles Malta

Future Focus is committed to the nine Data Protection Principles contained in the Data Protection Act Malta, being:

The data must be is processed fairly and lawfully

This quite simply means that one must always be sure that the processing of such data is done according to law and that it is only done where necessary.

The data must be processed in line with good practice

This entails that where the processing of personal data is necessary, that it be done in conformity with good working practice. To illustrate, a bank should only process personal data where it is necessary for it to perform its functions as a bank and should do so according to responsible banking practices.

That personal data is only collected for specific and explicit purposes which are legitimate.

This effectively means that whenever such data has to be collected, the data subject always has to be advised as to the reason for the data collection. Furthermore, the data always has to be collected for the sake of something specific and that must also be legal.

That personal data, once collected is not used for purposes incompatible with the reason for which it was collected.

This requires that the Data Controller always remain vigilant that the data collected is always being consistently used for the reasons which were explained to the data subject when the data was collected. This does not bar the Data Controller from using the information for other purposes entirely though as long as the necessary consent to do so is given by the data subject.

That the personal data collected is adequate and relevant to the purpose for which it was collected.

If one intends to make a database of telephone numbers for the sake of a marketing contact list, one should not need to ask for a person's I.D. card number. This means that one should only collect information that is relevant to the purpose for which it is needed. Any information which has no relation to the reason that other data is being collected should be avoided.

That no more personal data is processed than is necessary with regard to the reason for processing.

Similar to the previous principle, one should take a minimalist approach in the amounts of data that are used wherever necessary. While the previous principle mainly deals with issues of relevance, this one deals with the content that is being used. If for example, a group of companies in the financial services sector transferred information from one company to another related to a particular client, they should not pass on more information than is necessary for the reason the data was requested.

That personal data is always correct up to date.

It is one of the Data Controller's most important duties to make sure that the data that's being collected is kept up to date. This is less of a protective measure and more to ensure that where the information is used to render a service to the data subject that it is done efficiently. To illustrate, if a mobile phone operator has the wrong address of one of its clients, any invoices or personal information regarding that person's mobile phone related activities will likely find itself in the hands of a person who has no right to it. It would also mean that the Data Subject would not know he is due to pay.

That all reasonable measures are taken to complete, correct, block or erase data which is incomplete or incorrect, taking into consideration the purposes for which they are processed.

This principles ensures that as far as possible, the Data Controller will always show due diligence in correcting any data which is in some way flawed. One should notice that the law requires that reasonable measures must be taken. This means that there is an element of discretion where a court finds itself deciding whether the Data Controller performed his functions to standard. This likely considers the fact that it is difficult for the Data Controller to catch every inaccuracy or discrepancy with data at the moment it occurs. It may often even require that the Data Controller maintain a certain degree of contact with the Data Subject, particularly where he has a suspicion that any information is incorrect.

That personal data is never kept for a longer time than is necessary, depending always on the reason for which it is being processed.

This is particularly relevant where information is being collected for statistical purposes. If the data is being used for a study with a view to achieving a particular goal, once that target has been reached, the data has no more reason to be kept and should be destroyed unless there is some other reason to hold onto it. Naturally, as is common to all matters related to personal data under this law, the Data Subject always has to be informed where there is any change in the reason for which the data is being used. Furthermore, they would have to consent to the data being used for the new purpose.

4. Control of Personal Data

Future Focus Ltd's use of personal data is registered with the Information Commissioner; the Chief Executive is the named contact. We have a duty to keep our registration up to date, so you should contact the Chief Executive you are aware of any changes in processing activity. Personal data that Future Focus keeps will not be disclosed under the Freedom of Information Act. Future Focus suppliers and stakeholders will be told that Future Focus may be obliged under the Freedom of Information act to disclose certain information so that they can make a decision whether to work with us at the onset of their services.

Future Focus is the data controller of all personal data held and processed on its behalf.

The relevant Director or Manager will monitor the use and deletion of data and ensure that staff follows the eight principles of data protection.

Information will be kept in line with our data retention guidelines. All employees are responsible for ensuring that information is not kept for longer the necessary, and that the retention period complies with any legal and/or contractual requirements.

When a record containing personal data is to be disposed of this will be done as follows:

i. Paper documentation will be permanently destroyed by shredding or incinerating; and
ii. Computer equipment or media will have all personal data completely destroyed by reformatting and/or overwriting.

All employees will be committed to information security and management will provide clear directions on responsibilities and procedures. The following policies apply to all staff.

Internal and remote access to computerised information and host application software will be controlled by appropriate levels of password, granted to staff on a "need to know" basis, with authorisation from the relevant line Manager. Security of computer information will be

provided by automated backup routines, run daily on all sites and configured according to professional best practice.

The Chief Executive will support staff to ensure the following for information resources:

i. That personal data is readily accessible to authorised individuals;
ii. That plans and procedures are in place for the necessary long term archiving of specific record types for purposes of access;
iii. That clear guidelines are established for disclosure to and consultation by legitimately interested parties of personal information stored on paper or computerised media; and
iv. That procedures are put in place for identification and removal of inappropriate or unnecessary personal data stored on any Future Focus information system.

Future Focus is committed to maintaining high standards of security and confidentiality for information in our custody and control. Such information includes business information, trade secrets, know-how and personal data relating to customers and clients, our own employees and third party company representatives.

Access to our computer systems is restricted. It is controlled by passwords. When an employee logs into the computer system using a password, a record of the activities of that employee is automatically generated. This is why it is important not to share passwords and to keep passwords secure. The computer system will prompt you to change your password every 40 days.

If an employee thinks that his or her password may have been disclosed, it must be reported immediately for a new password to be issued.

5. Monitoring use of company IT

Employee use of Future Focus IT facilities is monitored to check compliance with this policy.

All employees are responsible for reporting any issues with IT computer systems or with security to the Chief Executive. Use of Future Focus IT computer systems is for Future Focus business purposes only. In particular employees must not load software or use cd-roms on company computer equipment as there is a risk that this could introduce viruses to the system and reduce system capacity.

Employees who have access to the internet are under a duty to use this facility for Future Focus business purposes only and in particular must not download games, or any material that would be considered unacceptable.

Company facilities may be used for private purposes in an emergency only and only with pior or immediate agreement with a senior manager.

Employees should be aware that emails are company documents, similar to using headed notepaper. In particular care must be taken to ensure that all outgoing emails include Future Focus's registration details, and that email is used appropriately and for work purposes only.

Emails are considered to be written documents and so they can evidence the making of a legally binding contract and their contents are subject to the laws of libel. Email should not be used to send personal data or documents containing personal data.

Paper records will be kept secure in a lockable cupboard.

Breach of the Information Security Policy, the IT Acceptable Use Policy or the Physical Security Policy is a disciplinary offence and could result in disciplinary action by Future Focus. Any employee, contractor or subcontractor who becomes aware of a data security breach shall immediately notify the known circumstances to Chief Executive.

If in doubt, you should report the incident. Other incidents may be reportable even if not included on this list. The following are examples of data security breach incidents:

i. Loss of a laptop which stores personal data;
ii. Loss of a memory or USB stick, CD-ROM or other portable storage device on which personal data is stored;
iii. System failure leading to loss or corruption of personal data;
iv. Errors in printing such as incomplete mail merging, or mismatching names and addresses;
v. Hacking attack; and
vi. Unforeseen circumstances such as a fire or flood.

The Chief Executive shall be responsible for:

i. coordinating external reporting of the breach to clients;
ii. putting together a team to handle the investigation and further reporting of the incident;
iii. investigating the incident;
iv. external reporting of the breach to regulators (see guidance from Information Commissioner about reporting serious incidents) and data subjects as appropriate;
v. liaison with external agencies in connection with the incident; and
vi. liaison with the press in connection with the incident.

The initial internal report of a data security breach by staff or contractors may be subject to the Future Focus whistle-blowing policy.

6. Data Protection Training

Training will be available to those who need it. Staff will be informed of their duty under the Data Protection Malta and will be expected to comply with the rules laid down in this policy. This will be followed up by an annual audit of data lists and staff will be expected to check and record the lists they hold. This will not excuse them from registering data bases as soon as they exist as per the eight principles.

There will be many purposes for collecting personal data, and at each point of collection it must be made clear to the person giving the information that Future Focus will hold the information only for specific purposes. In general the following declaration should be used on forms, on the website and in scripts where personal data is to be collected as part of the process data:

“The information supplied on this form will be used to keep you informed of community related matters by telling you about publications, conferences and seminars in relation to funding projects. We would also like to contact you by letter, email or telephone to advise you of these events. If you would like to be kept informed please tick here [ ]

Future Focus do not share their mailing lists with other organisations unless we advise you of it at the time of collecting your personal details."

The obligation when using data processors:

The Seventh Data Protection Principle requires appropriate technical and organisational security measures for personal data and this obligation applies when information is passed from Future focus (the “data controller”) to an outsource service provider who will process it on its behalf (the “data processor”). When the processing of personal data is outsourced, data controllers must take steps to ensure the reliability of their data processors both in the selection criteria for choosing a service provider and in subsequent monitoring of the provider"s performance.

In addition, the data controller must have a written contract with its data processor(s) which commit the data processor to act only on the instructions of the data controller and to adhere to the requirements of the Seventh principle when processing personal data on behalf of the data controller.

Examples of activities which are routinely outsourced and which will involve processing personal data by a data processor are:

i. Mailing house to distribute reports and accounts and circulars; and
ii. Payroll administration.

"To the extent that [the service provider] is a data processor within the meaning of the Data Protection Malta it hereby undertakes:

i. Only to act on instructions from [the client] when processing personal data on [the client's] behalf;
ii. To comply with the Seventh Data Protection Principle Malta in relation to the processing of personal data on [the client's] behalf;
iii. To ensure that equivalent obligations of security are imposed on any third party service supplier to [the service provider] ("subcontractors") which process personal data on behalf of [the client];
iv. To allow [the client] access to your premises during normal office hours to carry out security checks subject to reasonable notice being given and / or to report on security issues as may be required by [the client] from time to time.

7. Dealing with Requests for Information (Subject Access Requests)

All individuals who are the subject of personal data are entitled to:

i. ask what information we hold about them and why;
ii. ask how to gain access to it;
iii. be informed how to keep it up to date;
iv. have inaccurate personal data corrected or removed;
v. prevent us from processing information or request that it is stopped if the processing of such data is likely to cause substantial, unwarranted damage or distress to the individual or anyone else;
vi. require us to ensure that no decision which significantly affects an individual is solely based on an automated process for the purposes of evaluating matters relating to him/her, such as conduct or performance; and
vii. be informed what we are doing to comply with our obligations under the Data Protection Malta.

Future Focus will usually provide this information for free depending on the ease of accessibility, but may charge up to £10. If a formal request for access to personal data is received from a data subject it should be dealt with as quickly as possible, and a response provided within 40 days of receipt of a written request.

Personal information should only be released to the individual to whom it relates, the disclosure of such information to anyone else without their consent may be a criminal offence. When a request for information is received, care should be taken to ensure that the individual requesting information is doing so legitimately.

Future Focus acknowledges that public bodies such as government departments are subject to the requirements of the Freedom of Information Act 2000 and the Environmental Information Regulations. Future Focus will:

i. assist and cooperate with any public body to enable it to comply with its Information disclosure requirements;
ii. transfer to the relevant public body any Request for Information made under the FOIA that it receives as soon as practicable and in any event within two working days of receiving a Request for Information;
iii. provide the public body with a copy of all Information in its possession or power in the form requested within five working days of the public body requesting the Information;
iv. provide all necessary assistance as reasonably requested by the public body to enable it to respond to a Request for Information within the time for compliance set out in Section 10 of the FOIA or Regulation 5 of the Environmental Information Regulations, this is currently 20 days; and
v. not respond directly to a Request for Information unless expressly arequested to do so by the relevant public body.

The public body shall be responsible for determining at its absolute discretion whether any Information is exempt from disclosure under the FOIA or the Environmental Information Regulations.

Future Focus acknowledges that public bodies may, under the FOIA or the Environmental Information Regulations, be obliged to disclose Information:

i. without consulting with the Future Focus; or
ii. following consultation with Future Focus and having taken its views into account.

Future Focus will ensure that all Information produced in the course of delivering a contract for a public body or relating to the contract is retained for disclosure and shall permit the public body to inspect such records as requested from time to time.

All Future Focus staff, consultants and contractors responsible for procuring and/or creating any new information systems or modifying existing systems will be responsible for ensuring that those systems will comply with future Focus‟s Data Protection Policy Malta and Procedures.

8. Data Protection FAQs

What is data protection?

The holding, using and processing of personal data in Malta is regulated by the Data Protection Malta. In the broadest terms data protection is about confidentiality and security of personal data and giving individuals certain rights including the right to access information relating to them held by companies, government bodies, medical trusts etc.

Personal data is information about a living individual (the "data subject"). It includes names, addresses, telephone numbers, etc. as well as opinions, photographs and images recorded by CCTV. Data protection law applies to all records held on computer and to structured paper files (for example HR files held in alphabetical order are covered.)

The Data Protection Malta sets out minimum standards of behaviour when dealing with personal data. It also establishes the office of the Information Commissioner, a regulator and ombudsman for information management generally, covering personal data, marketing and privacy issues and Freedom of Information.

When does data protection apply to businesses?

Information relating to corporate bodies is not "personal data" for the purposes of Data Protection Malta law because a company is not a living individual. However, information relating to individual contacts at client offices, suppliers, members and visitors constitutes personal data as does information relating to sole traders and partnerships.

Information relating to colleagues at work is one of the largest and most commonplace areas involving the processing of personal data.

What is Notification?

Organisations are required to notify or register for data protection unless they are exempt. Some organisations are required to register simply by virtue of their activities which are primarily data management businesses, such as pension scheme administrators, lawyers, consultants and marketing firms. Organisations that supply goods or services where data management is a more peripheral activity do not need to register.

Certain ancillary activities may mean that an exempt body still has to register.

If it is responsible for a CCTV scheme, if it promotes goods or services on behalf of third parties, if it markets other companies" goods and services or if it uses credit reference information, it must register.

What are the Data Protection principles?

When using personal data relating to colleagues, consumers and representatives of other companies, organisations are required to act in accordance with the Data Protection Principles Malta. These are set out in the Data Protection Policy & Procedures Malta with explanatory notes of how they apply in a work context.

What access rights are there to personal data?

Organisations are under a legal obligation to allow a "data subject" (the individual about whom personal data is held) access to the information relating to them on computers and in some manual files. There is a limited period (40 days) in which to respond to a *data subject access request*.

What other data protection rights are there?

Individuals have other rights under the Act relating to the way in which their personal data is processed. In particular, individuals have the right to object to the use of their personal data for direct marketing purposes. If this right is exercised, the organisation has no option but to cease using that individual"s personal data for direct marketing. Organisations must ensure that they can identify when this right is being exercised and that they can stop future direct marketing on request.

Data Protection issues usually arise in connection with a complaint or grievance, identifying the data protection aspect of these complaints quickly will help to resolve them within the time limits set down by law.

How might data protection law affect you personally?

Data Protection Malta law has always carried penalties for individuals (as well as organisations and their key officers) who breach the provisions. These are some areas to consider.

The unauthorised obtaining or disclosure of personal data is a criminal offence. As a minimum, you should always check that anyone requesting information has the right to access it. Think twice before giving out contact details on request. As a rule, never give out home contact details. Instead, offer to contact the person yourself and ask them to contact the enquirer. Take particular care on the telephone when you may feel under pressure to respond quickly to an enquiry, you can always offer a callback when you have sorted out the correct response.

Personal data should be treated confidentially and not used for any purpose other than communication and activities related to business affairs. In addition personal data should be kept secure, which means putting files away in cabinets in the evening and if you take a break during the day. Screen savers should be activated and PCs sited so as to minimise the chance of information on screen being looked at by others. Apply good housekeeping rules to laptops too, they should be kept safe and the absolute minimum of personal information should be kept on the hard drive.

The hard drive should be backed up regularly if there is no dial-in facility.

In general you should treat other people's personal data as you would want them to treat your own.

Remember also that normal legal rules such as libel apply to written documents. Therefore do not include opinions or personal comments on file (and email) which the data subject might find offensive. The individual has the right to access that information, including your opinion.