Data Security Policy

Effective 1st January 2018 – GDPR added 25th May 2018

Data Security Policy

1 Introduction

1.1 The Data Protection Act 1998 ('the Act') imposes certain obligations upon Sypro Management Ltd. Limited in relation to the processing of personal data. These obligations are contained within eight data protection principles. The seventh principle relates to data security and requires us to take appropriate technical and organisational measures to safeguard personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage. For more information on the other principles please refer to the Data Protection Policy.

1.2 We recognise the importance of personal data to our business and the importance of privacy rights to individuals about whom we process personal data. This Policy is intended to assist our staff to comply with the requirements of the seventh principle. This Policy is not limited to protecting personal data but extends to all information which we hold. References to 'personal data' should be read to include information of any kind that is used within the business, including confidential information.

1.3 The Act includes a number of defined terms which are used in this Policy. These terms are:

1.3.1 'data subjects' means individuals about whom we process personal data;

1.3.2 'personal data' means data which relate to a living individual who can be identified from those data or from those data and other information which is in our possession, or likely to come into our possession;

1.3.3 'processing' means virtually anything we do with personal data such as collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction;

1.3.4 'sensitive personal data' means personal data about an individual's racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; membership of a trade union; physical or mental health or condition; sexual life; commission or alleged commission of an offence; or the proceedings relating to any alleged or actual offences, the disposal of such proceedings or the sentence of the court in such proceedings.

*References to 'we' and 'us' refer To Sypro Management Ltd. Limited.

2 Your Responsibilities

2.1 You must familiarise yourself with this Policy and implement its requirements within your department and working practices. Please refer to the Data Protection Policy for guidance on the requirements of the Act in general. You can obtain a copy of the Data Protection Policy from the Human Resources Department.

2.2 Under the terms of your employment contract with Sypro Management Ltd. Limited you have an obligation to comply with this Policy.

Any failure to comply with this policy may be a disciplinary offence which could result in summary dismissal. Negligent or deliberate breaches could result in criminal liability for you personally.

3 Policy

3.1 The seventh data protection principle requires Sypro Management Ltd. Limited to take appropriate technical and organisational measures to protect personal data against unauthorised or

Data Security Policy

unlawful processing, accidental loss, destruction, or damage.

3.2 In order to assist us to comply with the seventh principle:

3.2.1 you must comply with the technical and organisational measures set out in the Annex to this Policy whenever you process personal data;

3.2.2 you must consider the nature of the personal data you are processing and determine whether the technical and/or organisational measures are commensurate to the harm that might result if there were a security breach. If the data are also confidential or sensitive personal data, an additional level of security will be required:

(a) Examples of confidential information may include (HR data (e.g. employee records, payroll data); financial information (e.g. bank account and/or credit card details);

(b) Examples of sensitive personal data may include (information about an individual's racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; physical or mental health or condition; sexual life; commission or alleged commission of an offence; or the proceedings relating to any alleged or actual offences, the disposal of such proceedings or the sentence of the court in such proceedings);

3.2.3 you should only hold personal data for as long as it is required for the purpose for which those data were originally collected. Once the data are no longer required, you must destroy or delete those data securely;

3.2.4 you must immediately report all actual or suspected security breaches to Gerard Toplass). Where the breach involves personal data, you should also notify the Data Protection Officer or Gerard Toplass.

3.3 Sypro Management Ltd. Limited is responsible for taking reasonable steps to ensure the reliability of employees who have access to personal data. If you are responsible for the recruitment of staff (whether permanent, temporary or contract), you must assist us to comply with this requirement by:

3.3.1 screening/vetting all new staff;

3.3.2 ensuring all new staff sign terms and conditions which include confidentiality and security obligations;

3.3.3 taking up references for all new staff;

3.3.4 ensuring new staff are trained on the care and handling of personal data when they join (eg as part of their induction training).

3.4 As part of Sypro Management Ltd. Limited's obligation to ensure the reliability of employees who have access to personal data, we must provide training on the requirements of the Act. If you are responsible for training staff (whether permanent, temporary or contract), you must ensure that periodic training sessions (including refresher courses) are provided to staff on data protection topics, including the care and handling of personal data and security requirements.

3.5 Sypro Management Ltd. Limited is required to take additional security measures whenever it uses third parties to process personal data on its behalf. Third parties may include (IT contractors, providers of hosting services for our websites, outsourced service providers, payroll providers, computer maintenance providers, disaster recovery service providers). These third parties are referred to as 'data processors'. If you are responsible for the selection or appointment of any data processors, or are involved in contract negotiations with data processors:

3.5.1 you must make sure you only select data

processors that provide sufficient guarantees in respect of the technical and organisational security measures they will use in relation to the processing of personal data. One of the ways in which you can achieve this is by requiring all processors to complete our Questionnaire for Prospective Data Processors. This questionnaire is designed to help you identify suitable processors and comply with the requirements of the Act;

3.5.2 you must enter into a contract in writing with each data processor. It is important to do this before the processing actually begins. If you are responsible for negotiating or drafting commercial contracts, please use one of our standard data processor contracts.

3.5.3 you must ensure that each processing contract makes it clear that data processors must only act on instructions from Sypro Management Ltd. Limited. We are responsible for the processing of all personal data, even if it is carried out on our behalf by a data processor. We must, therefore, maintain control over such processing at all times;

3.5.4 you must ensure that each data processor agrees to take appropriate technical and organisational measures to protect any personal data that it processes on our behalf from unauthorised or unlawful processing, accidental loss, destruction or damage. It is important that we specify any measures that must be taken;

3.5.5 you must ensure that we have the right to check the data processor's compliance with the terms of any processing contract. This may involve auditing the data processor from time to time to make sure that it is processing in accordance with our instructions and the security measures we have specified, as well as any other data protection related requirement of the Act;

3.5.6 if the data processor will be holding personal data on our behalf and we do not also have a copy of those data, we must make sure the processing contract includes a provision that requires the processor to assist us promptly with any *subject access request we might receive in relation to any of the data held by the data processor; *A 'subject access request' is a request received from a data subject asking for access to personal data which we process about him or her

3.5.7 you must ensure that upon termination of the processing contract, the processor promptly returns or destroys the personal data as directed by us;

3.5.8 if the data processor will be collecting personal data on our behalf, the processing contract must include an obligation upon the processor to give our data protection notice (which the processor is not allowed to modify) to all individuals about whom the processor collects personal data.

3.6 If the data processor proposes to use sub-processors to assist with the processing services, you should seek advice from the Data Protection Officer or Gerard Toplass as this will have consequences for Sypro Management Ltd. Limited and specific provisions will need to be included in the processor agreement.

3.7 It is important to remember that just because we delegate some our processing activities to a data processor does not mean that we can delegate our responsibility to comply with the Act.

4 Contacts And Responsibilities

4.1 If you have any queries about this Policy, please contact the Data Protection Officer or Gerard Toplass.

4.2 We reserve the right to change this Policy from time to time to take into account any relevant changes in law or guidance from the Information Commissioner.

Data Security Policy

Changes made to this Policy will be notified on the HR intranet or posted on staff bulletin boards or within the staff forum meetings.

Issue No. 1 – January 2013

Annex
Technical And Organisational Measures

Technical Security Measures

1 Protection against malicious software/ viruses (eg software should not be installed from removable media or downloaded from the internet without virus checking it first)
2 Backing up data (eg daily back ups should be taken of all data on our systems; data should not be stored on local drives or removable media as these will not be backed up)
3 Encryption
4 Secure exchange of information
5 User access controls (eg passwords should be allocated to all users; passwords should be changed on a regular basis; passwords should not be pinned up next to the computer or anywhere else where they could be seen; computers should have password activated screen savers that can be turned on whenever the user is away from his or her desk; passwords should include a mixture of letters and numbers; avoid passwords that are easy to guess such as your name or date of birth; different access should be allocated to different users depending on job description and need to access personal or confidential data; different access rights should be allocated to individuals who have a need to modify personal or confidential data; read and write privileges should be allocated depending on job description and need)
6 Network access controls (including passwords)
7 Monitoring system access and use
8 Guidance on mobile computing (eg do not leave laptops unattended in cars or in public places or on top of desks left unattended overnight)
9 Guidance on teleworking (eg do not use your home computer for work purposes unless you have

CCTV Policy

1 Introduction

1.1 Sypro Management Ltd. Office Equipment Limited has decided to use closed circuit television ('CCTV') within and around its business premises for the purpose of crime prevention and public safety. References to 'we' and 'our' in this Policy are references to Sypro Management Ltd. Limited).

1.1 Our use of CCTV may result in the processing of images that can identify specific individuals in such a way that they are covered under the Data Protection Act 1998 ('the Act'). This will happen where the information captured by the CCTV scheme falls within the definition of 'personal data'. It is important to understand what is meant by this definition as the Act will only apply where our CCTV system is processing personal data.

1.2 The Act defines 'personal data' as data which relate to a living individual who can be identified from those data or from those data and other information which is in our possession, or likely to come into our possession. For example: If you answer YES to ALL of the following questions this will indicate that we are processing personal data and our CCTV scheme is covered by the Act:

Personal data-checklist – tick Yes/No

(a) Are CCTV images clear enough to identify particular individuals and what they are doing?

(b) Are individuals the focus of the CCTV images?

(c) Do the CCTV images tell us something about particular individuals? (ie do we learn about individuals' activities as a result of the CCTV images?)

If you answer NO to ALL of the following questions then this will indicate that we are not processing personal data and our CCTV scheme is not covered by the Act:

Personal data-checklist – tick Yes/No

(a) Do you ever operate the cameras remotely in order to zoom in/out or point in different directions to pick up what particular people are doing?

(b) Do you ever use the images to try to observe someone's behaviour for your own business purposes such as monitoring staff members?

(c) Do you ever give the recorded images to anyone other than a law enforcement body such as the police?

1.4 Therefore, if our CCTV scheme is recording a general scene without any incident occurring and with no focus on any particular individual's activities, these images are unlikely to be covered by the Act.

1.5 The Act also defines the word 'processing' to mean virtually anything we do with personal data such as collection, modification, transfer, viewing, deleting, holding, backing up, archiving, retention, disclosure or destruction.

2 Your Responsibilities

2.1 All employees (including temporary and contract staff) who are responsible for implementing, managing, operating or using the CCTV scheme must do so:

2.1.1 only as authorised and in accordance with this Policy;

2.1.2 with respect for those individuals who are being monitored;

2.1.3 for the limited purposes described at the start of this Policy and for no other purpose.

For general guidance on the requirements of the Act, please refer to the Data Protection Policy. Copies can be obtained from the HR Department.

CCTV Policy

2.2 Under the terms of your employment contract with Sypro Management Ltd. Limited you have an obligation to comply with this Policy.

Any failure to comply with this policy may be a disciplinary offence which could result in summary dismissal. Negligent or deliberate breaches could result in criminal liability for you personally.

3. Initial Assessment

3.1 Before installing the CCTV scheme, we carried out an initial assessment to determine several factors which are relevant to our compliance with the Act. Our initial assessment concluded as follows:

Impact Assessment--findings

(a) The purposes for the CCTV scheme are: (specify the purposes)

(b) The personal data processed by the CCTV scheme are: (specify, eg images of our employees, customers, the public in and around our office premises, car parks)

(c) The legal basis for the processing of personal data by the CCTV scheme is: (specify the relevant schedule 2 or 3 conditions under the first data protection principle)

(d) The individuals who will be responsible for the management and operation of the CCTV scheme are: (specify either by role or name)

3.2 Our notification to the Information Commissioner must include the purpose(s) for which the CCTV scheme will be used. You must contact the Data Protection Officer or Gerard Toplass with details of any CCTV scheme and they will check our notification to ensure it accurately reflects our processing.

4. Siting The Camera

4.1 The position of the CCTV cameras is critical to ensuring our compliance with the Act. You must apply the following principles whenever you are siting cameras:

Siting the cameras-checklist – tick Yes/No

(a) Cameras should be restricted to monitor only those areas which are intended to be monitored

(b) Cameras should not be used to monitor any adjoining areas which are not intended to be covered by the scheme (such as gardens or private dwellings)

(c) Where cameras are adjustable, they should be restricted so that they cannot be adjusted to overlook areas outside the CCTV monitored site

(d) Cameras should be positioned to record images which are relevant to the purposes for which we run the scheme

5. Signage

5.1 The Act requires that we notify individuals of the purposes for which their personal data may be processed. Where a CCTV scheme is in operation, we must comply with the requirements set out below.

Signage requirements-checklist – tick Yes/No

(a) Signs must alert individuals they are entering a CCTV monitored zone

(b) All signs must be legible and visible

(c) The size of the sign will depend on the location and how visible it is to individuals

(d) All signs must include the following information:

-- the identity of the person responsible for the scheme (ie (name of data controller))

CCTV Policy

-- a description of the purpose(s) of the scheme (refer to paragraph 3.1(a))
-- details of who to contact regarding the scheme

5.2 The Information Commissioner has recommended the following wording: Images are being monitored for the purposes of crime prevention and public safety. This scheme is controlled by Sypro Management Ltd. Limited. For further information contact 01482 323235.

5.3 Where an image of a camera is used on the sign, the notice can be shortened to: This scheme is controlled by Sypro Management Ltd. Limited. For further information contact 01482 323235.

5.4 We must notify employees if they will be monitored by CCTV. This notification may be provided on application forms and in the employee handbook.

6. Quality of Images

6.1 Images produced by the CCTV scheme must be as clear as possible to enable us to use those images for the purpose for which they were obtained. For example, if we are using the CCTV scheme for crime detection and prevention purposes, the images must be clear enough to identify individuals and be used in evidence. The CCTV scheme must comply with the following quality requirements:

Quality of CCTV images-checklist – tick Yes/No

(a) CCTV equipment must be checked, maintained and cleaned regularly to ensure it functions properly and clear images are recorded. A record of any maintenance work should be retained

[(b) Only good quality tapes should be used to record images. Tapes should be replaced regularly

[(c) Avoid recording images over previously recorded images which degrades the picture quality

(d) Cameras should not be used if they produce poor or deteriorated CCTV images. Damaged cameras should be sent promptly for replacement or repair and be returned within specific time limits

[(e) The data and time on the CCTV scheme should be periodically checked to ensure they are accurate

(f) Consider any physical conditions that may be an issue at the CCTV site and put in effect any remedial actions to address those issues

(g) Consider whether it is necessary to record in real time on a continuous basis, or whether to limit monitoring activities to certain times of the day

7. Processing The Images

7.1 The Act prevents us from keeping CCTV images for longer than necessary for the purposes for which those images were recorded. Bearing in mind the purpose(s) for which Sypro Management Ltd. Limited is operating the CCTV scheme, we have determined that the following retention periods shall apply:

Purpose Retention period

(list all purposes and set out corresponding retention periods, eg:) public safety 60 days evidentiary purposes until such time as the proceedings have been determined 6.2

7.2 Once the relevant retention period has expired, we must securely destroy or erase the images.

7.3 We must maintain the integrity of all images whilst they remain in our possession so that the

evidentiary value of those images is protected. It is important that we process the CCTV images in accordance with the following requirements:

Processing of CCTV images--checklist – tick Yes/No

(a) CCTV images should be kept in a secure place to which access is controlled (this is particularly important where images are used for evidentiary purposes)
(b) Where images are used for legal proceedings, you must keep a record of:
-- the date on which the images were removed from the CCTV scheme
-- the reason for the removal
-- any crime incident number to which the images relate
(if any)
-- the current location of the images
-- the signature of the collecting police officer (if any)
(c) Where the CCTV scheme records images from areas that individuals would expect to be private (eg rest rooms), these images should only be viewed by restricted and authorised employees
(d) Access to CCTV images should be restricted to authorised employees who will decide whether to allow requests for access by third parties
(e) Viewing of recorded images should take place in a restricted area (eg the office of an authorised employee). Access to such area should be restricted whilst viewing is taking place
(f) Where the medium upon which CCTV images are recorded is taken for viewing purposes, a record should be kept of the following:

-- the date and time of removal
-- the name of the person removing the images
-- the name of the person viewing the images
-- the reason for the viewing

(g) All employees responsible for managing, operating or otherwise using CCTV must be trained in connection with this Policy

8. Access To And Disclosure Of Images To Third Parties

8.1 Access and disclosure of CCTV images must be restricted to ensure privacy rights of individuals are respected and the evidentiary value of the images is maintained. Any disclosure of personal data must comply with the Act. This means we must have a lawful ground to justify that disclosure (see paragraph 3.1(c) above). The following principles must be applied in relation to access and disclosure:

Access and disclosure-checklist – tick Yes/No

(a) Only authorised employees should be granted access to CCTV images and only to the extent necessary for the purposes for which the images were recorded
(b) CCTV images should only be disclosed to third parties where the disclosure is necessary for any of the purposes for which the images were recorded (as set out in paragraph 3.1(a))
(c) A record should be kept of all requests for access or disclosure, together with any reasons for refusing a request
(d) If access or disclosure is allowed, the following should be recorded:
-- date and time of access/ disclosure
-- identity of person who was given access/ disclosure
-- reason for allowing access/ disclosure
-- extent of information which was accessed/ disclosed

-- the outcome, if any, of the viewing
-- the date and time the images were returned

(e) Recorded images should only be made available as set out in this Policy

(f) If the decision has been taken by a senior manager to disclose CCTV images to the media, any images of individuals should be blurred or disfigured so they cannot be identified

8.2 The most frequent requests for disclosure are likely to come from third parties (such as the police or government agencies). A request for disclosure could be made for any reason. However, the most common reasons are in relation to crime prevention purposes or where there is a statutory purpose for the disclosure:

Disclosures for the crime prevention purposes--checklist – tick Yes/No

(a) Where the disclosure is requested for the purpose of preventing or detecting crime, apprehending or prosecuting offenders, or assessing or collecting tax (the crime and taxation purposes) we must:
-- ask the third party to justify its request for the CCTV images
-- ask the third party to confirm that a failure to make the disclosure would be likely to prejudice any of the crime and taxation purposes
-- if the request appears justified, we may choose to disclose the images (as long as the request is in writing, signed by a senor police officer)
-- any decision to disclose must be on a case-by-case basis and a record of all disclosures must be kept.

Disclosures for statutory purposes--checklist – tick Yes/No

(b) Where the request for disclosure is made under a statutory provision (other than the Act):
-- we must disclose the CCTV images if the statutory provision imposes upon us a mandatory duty to disclose
-- we can choose whether or not disclose the CCTV images if the statutory provision imposes upon us a discretion as to whether or not to disclose
-- any decision to disclose must be authorised by a senior manager

9. Access By Individuals And Other Rights

9.1 Individuals have a right to access personal data which we process about them, which includes (in most cases) CCTV images of them. If you receive a request for access, please refer it promptly to the Data Protection Officer or refer to the Subject Access Policy for further guidance.

9.2 Where CCTV images reveal other individuals, we must blur or disfigure the faces of those other individuals so they are not recognisable. If our CCTV scheme does not have the ability to do this, you should ask the editing agency to do it on our behalf.

9.3 If a decision is made not to grant subject access to some or all of the CCTV images, you should record the reason for reaching this conclusion, details of the request (including the date it was made), and the name of the person who made the decision not to provide subject access.

9.4 In addition to the right of access, an individual also has the right to ask us to stop processing his personal data where this is likely to cause substantial and unwarranted damage to him or

her. If we receive such a request we have 21 days in which to respond with our decision. You should ensure that all decisions are documented, a record is kept of all requests and our response to that request.

10. Covert Monitoring

10.1 In certain limited and exceptional cases, we may be required to carry out covert monitoring (ie use the CCTV scheme to monitor individuals without alerting them to the fact). Covert monitoring should only take place once the following factors have been considered and a decision has been reached that it is appropriate not to notify the individuals of the monitoring:

Covert monitoring--checklist – tick Yes/No

(a) The purpose for the monitoring must be in respect of identified and specific criminal activity

(b) The monitoring must be necessary in order to obtain evidence of that criminal activity

(c) The use of signage must be likely to prejudice the purposes for the covert monitoring (ie the success of obtaining evidence of a criminal activity)

(d) The covert monitoring should only take place over a specific time period and should not continue after that time period has expired or the investigation has ended

(e) Any monitoring which is likely to be oppressive must be limited (eg an individual's office) unless there are overriding reasons for doing so

(f) Covert monitoring should not be used in areas where individuals expect privacy (such as rest rooms) unless there is a real suspicion of serious crime and an intention to involve the police

(g) Covert monitoring should be authorised by a senior manager

(h) Any information that is not relevant to the main purpose of the covert monitoring (ie detecting and preventing criminal activities and unlawful acts) should be disregarded and, where possible, deleted

10.2 Any third party appointed on behalf of the business to collect information about individuals covertly will be data processors. We must ensure that we have a contract in writing with such third party under which they agree to act only in accordance with our instructions. See further the Data Security Policy for a description of the types of provisions that should be included in processing agreements.

11. Contacts And Responsibilities

11.1 If you have any queries about this Policy, please contact the Data Protection Officer or your manager.

11.2 We reserve the right to change this Policy from time to time to take into account any relevant changes in law or guidance from the Information Commissioner. Changes made to this Policy will be notified on the HR intranet or posted on staff bulletin boards or announced in the staff forum meetings.

Data Protection Policy

Sypro Management Ltd. Limited is committed to ensuring its compliance with the requirements of the Data Protection Act 1998 ('the Act'). We recognise the importance of personal data to our business and the importance of respecting the privacy rights of individuals. This Data Protection Policy ('the Policy') sets out the principles which we will apply to our processing of personal data so that we not only safeguard one or our most valuable assets, but also process personal data in accordance with the law.

It is the responsibility of all our employees to assist Sypro Management Ltd. Limited to comply with this Policy. In order to help employees comply, we have produced a Data Protection Guidance document ('the Guidance') which explains in more detail the requirements of the Act. Employees must familiarise themselves with both this Policy and the Guidance and apply their provisions in relation to any processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to summary dismissal. Serious breaches could also result in personal criminal liability.

In addition, a failure to comply with this Policy could expose the business to enforcement action by the Information Commissioner (which could result in restrictions being imposed on our use of personal data) or to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

For these reasons, it is important that all employees familiarise themselves with this Policy and the Guidance, and attend all training sessions in respect of the care and handling of personal data.

Data protection principles
Sypro Management Ltd. Limited will comply with the following principles in respect of any personal data which it processes as a data controller:

1 Personal data must be processed fairly and lawfully and must not be processed unless:

1.1 at least one of the conditions in Schedule 2 to the Act is met; and

1.2 in the case of sensitive personal data, at least one of the conditions in Schedule 3 to the Act is also met.

The Schedule 2 and 3 conditions are set out in the Guidance.

1.3 Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with those purposes.

1.4 Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

1.5 Personal data must be accurate and, where necessary, kept up to date.

1.6 Personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes.

1.7 Personal data must be processed in accordance with the rights of data subjects under the Act. These rights are:

1.7.1 the right of subject access;

1.7.2 the right to prevent processing likely to cause damage or distress;

1.7.3 the right to prevent processing for purposes of

Data Protection Policy

direct marketing;

1.7.4 the right to object to automated decision-taking.

1.8 Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

1.9 Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This Policy may be amended from time to time to reflect any changes in legislation. Any queries should be directed at the Data Protection Officer or Gerard Toplass.

Data Protection Policy Guidance Note

Introduction

This Guidance Note ('the Guidance') forms part of the Data Protection Policy and provides supplementary information to enable employees to better understand and comply with the Data Protection Policy. Sypro Management Ltd. Limited is required to comply with the Data Protection Act 1998 ('the Act') in respect of its processing of personal data (such as information about our customers, employees and suppliers). It is important for all employees to familiarise themselves with both the Data Protection Policy and this Guidance so that any processing of personal data can be carried out in accordance with the Act. Failure to do so may expose Sypro Management Ltd. Limited to enforcement action by the Information Commissioner (which could result in restrictions being imposed on our use of personal data) and/ or to complaints and/or claims for compensation from affected individuals. There may also be negative publicity as a result of a breach.

You are required to assist Sypro Management Ltd. Limited to comply with its obligations under the Act. In order to do this you must comply with the Data Protection Policy and this Guidance whenever you process personal data, as well as any other data protection related policy that may be applicable to your area of work. Any failure to comply with this policy may be a disciplinary offence which could result in summary dismissal. Negligent or deliberate breaches could result in criminal liability for you personally.

Any questions about this policy should be raised with the Data Protection Officer or Gerard Toplass.

Legal Frameworks

The Act sets out eight data protection principles which must be followed in relation to all processing of personal data. These principles are set out in the Data Protection Policy and are reproduced below, together with an explanation of what they require. Sypro Management Ltd. Limited processes personal data about a wide range of data subjects, such as employees, customers, members and suppliers. We process personal data for a number of purposes, such as administration, marketing, profiling our customers and credit checking. It is critical to our business that we are able to use personal data in this way. In order to continue to be able to do so, we must ensure compliance with the principles set out in the Act.

Definitions
In order to fully appreciate the requirements of the Act it is important for you to understand the meaning of certain key words and phrases which are used within the Act. These are set out below:

1.1 Data--is information that is processed electronically (eg by computer); is recorded manually (eg on paper) with the intention of being processed electronically; is recorded as part of a relevant filing system (see below); or is none of these but forms part of an accessible record;

1.2 Data controller--is the organisation that determines the purposes for which and the manner in which personal data are processed. Sypro Management Ltd. Limited is the data controller. Employees, managers, contractors and other staff are not data controllers;

1.3 Data processor--is an external organisation that

Data Protection Policy Guidance Note

we appoint to process personal data on our behalf. Examples of these might include our security services and gatehouse workers, our IT outsourced services provider or our external payroll bureau;

1.4 Data subject--is a living, identifiable individual about whom we process personal data;

1.5 Information Commissioner--is the supervisory authority responsible for enforcing the provisions of the Act in England and Wales;

1.6 Personal data--are data which relate to a living individual who can be identified from those data or from those data and other information which is in our possession or likely to come into our possession. Personal data include opinions and indications of our intentions towards an individual;

1.7 Processing--has a wide meaning and covers virtually anything that can be done in relation to personal data, such as obtaining, recording, holding, altering, retrieving, consulting, using, disclosing, blocking, erasing or destroying personal data;

1.8 Relevant filing system--is a set of manual information (ie paper files) relating to individuals which is structured by reference to individuals or criteria relating to them in such a way that specific information relating to a particular individual is readily accessible;

1.9 Sensitive personal data--means information as to (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) his trade union membership, (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, and (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The Principles
First principle
Personal data must be processed fairly and lawfully and must not be processed unless (a) at least one of the conditions in Schedule 2 is met and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

This is the first and possibly most important of all the principles. It requires us to process personal data fairly and lawfully. Each of these requirements is considered in turn below.

Lawful processing
The Act prohibits the processing of any personal data unless that processing can be justified under one of a number of conditions which are set out in Schedules 2 and 3 of the Act. It is worth remembering the very broad definition of 'processing' which includes obtaining, disclosing, using and viewing.

You must justify your processing of all personal data under one of the conditions set out in Schedule 2. If you cannot find a condition that justifies your processing then that processing may not take place.

Schedule 2 conditions

1 The data subject has given his consent to the processing.

2 The processing is necessary in order to enter into or perform a contract with the data subject.

3 The processing is necessary for compliance with any legal obligation to which Sypro Management

Data Protection Policy Guidance Note

Ltd. Limited is subject (other than an obligation imposed by contract).

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary for the (a) administration of justice, (b) exercise of any functions conferred on any person by or under any enactment.

6 The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

When considering the above conditions remember the broad definition of processing. For example, obtaining consent to processing means obtaining consent to the disclosure, collection, use, destruction etc of personal data.

In addition, where you are processing sensitive personal data, you must also justify that processing under one of the conditions in Schedule 3. This is a safeguard which recognises the sensitive and sometimes confidential nature of this category of personal data. The most relevant Schedule 3 conditions are set out below.

Schedule 3 conditions

1 The data subject has given his explicit consent to the processing.

2 The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on Sypro Management Ltd. Limited in connection with employment.

3 The processing is necessary (a) in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject, or (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4 The processing (a) is necessary for the purposes of, or in connection with, any actual or prospective legal proceedings, (b) is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

5 The processing is necessary for the (a) administration of justice, (b) exercise of any functions conferred on any person by or under any enactment

6 The processing is necessary for medical purposes and is undertaken by (a) a health professional or (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

7 The processing (a) is of sensitive personal data consisting of information as to racial or ethnic origin, (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

8 The processing (a) is in the substantial public interest, (b) is necessary for the purposes of the prevention or detection of any unlawful act, and (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

9 The processing (a) is of sensitive personal data

Data Protection Policy Guidance Note

consisting of information as to religious beliefs or other beliefs of a similar nature; or physical or mental health or condition, (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons holding different religious beliefs; or different states of physical or mental health or conditions, with a view to enabling such equality to be promoted or maintained, and (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and (d) does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

10 The processing (a) is in the substantial public interest, (b) is necessary for research purposes, (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject, and (d) does not cause, nor is likely to cause, substantial damage or distress to the data subject or any other person.

Remember: unless you can justify your processing of sensitive personal data under both Schedules 2 and 3, you may not process those data.

Fair processing

The second requirement of the first principle is that personal data must be processed fairly. In broad terms what this means is that we must ensure transparency of processing so that data subjects are aware of who is processing their personal data and why. We achieve this by giving data subjects a data protection notice which meets the following requirements:

Content of data protection notice:

1. the identity of the data controller (ie Sypro Management Ltd. Limited)
2. the purposes for the processing (if one of those purposes is marketing then we should include a description of the communication channels that we intend to use and offer the data subject an opportunity to object. If any of those channels involve marketing by email, SMS, fax or automated calling systems, we need (as a general rule) to obtain the data subject's consent)
3. any other information that is necessary to make the processing fair (such as any recipients of the data and their purposes, a reminder of the data subject's right of access and correction and whether any of the information we are asking for is mandatory or voluntary)

Timing of data protection notice:

4. The data protection notice must be given to the data subject at the right time. Where we obtain personal data directly from the data subject (eg as a result of a telephone call, or online journey) we must give the notice to the data subject at the time we obtain his data
5. Where we obtain personal data about a data subject from a third party source (eg a family member or a list rental provider) we must provide the data protection notice as soon as reasonably practicable after we have started processing his data (unless it would be a disproportionate effort to do so)

Position and format of data protection notice:

6. The data protection notice must be reasonably prominent and in reasonably legible font
7. The data protection notice must be included at every point where we collect personal data, such as application forms, websites, medical reports, appraisals
8. If, for example, the data protection notice is provided online, it must be positioned so that it

Data Protection Policy Guidance Note

can be seen and not hidden behind a hypertext link

You can obtain copies of our standard and current data protection notices from the Data Protection

Officer or Gerard Toplass. These notices have been drafted to take account of the kind of processing that we do. You should use the data protection notices whenever you obtain personal data. You must not modify any of these notices without prior authority. These notices have been drafted so that they comply with the Act and any modification on your part could change that. If you think the notices do not cover your particular processing activities you must discuss this in the first instance with the Data Protection Officer or Gerard Toplass.

Second principle
Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with those purposes.

The second data protection principle sets out two requirements:

9. personal data must be obtained only for one or more specified and lawful purposes. Our data protection notices will specify the purposes for which we will process personal data and we are not permitted to process those data for a new purpose (unless the data subject gives his consent). Furthermore, we have an obligation to register our processing activities with the Information Commissioner and this requires that we provide a description of all the purposes for which we process personal data. If we want to process personal data for a new purpose, we need to notify the Information Commissioner.
10. personal data must not be further processed in any manner incompatible with the purpose or purposes for which the data were obtained. A breach of this principle could also result in a breach of the first principle. For example, if a data protection notice describes the purposes for which personal data will be used as administration, marketing and risk assessment, we should not use those data for any other purposes, unless those additional purposes would be totally obvious to the individual. To do otherwise could result in unfair processing in breach of the first principle and a breach of the second principle.

Third principle
Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

The third data protection principle requires that personal data must be adequate, relevant and not excessive. You must, therefore, ensure:

11. you identify the personal data needed for a particular purpose and you collect the minimum amount required to properly fulfil that purpose;
12. you do not hold personal data on a ‘just- in-case’ basis because you think it might be useful in the future but without having any clear idea of what that future purpose might be;
13. you keep data up to date (or else data which were originally adequate may cease to be so);
14. you do not keep data for too long (otherwise those data may cease to be relevant and become excessive).

Fourth principle
Personal data must be accurate and, where necessary, kept up to date.

Personal data will be inaccurate if they are

incorrect or misleading as to any matter of fact (eg an incorrect name or address). If you are inputting data onto our system and are unsure as to the accuracy of certain information (e.g. because you cannot read the handwriting or because it looks like an obvious mistake or omission), you should try to get in touch with the data subject to clarify the issue. We will not be in breach of this principle, even if we are holding inaccurate data if:

15. we accurately recorded those data when we received them from the data subject or a third party and;
16. we took reasonable steps to ensure the accuracy of those data and;
17. if the data subject has notified us that the data are inaccurate, we have taken steps to indicate this fact (e.g. by making a note that we have received an objection).

You must take reasonable steps to keep data up to date to the extent necessary. The purpose for which data are held will determine whether they need to be kept up to date or not. For example, historical records of transactions should not, as a general rule, be updated.

Fifth principle
Personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes.

You should review the personal data which you hold on a regular basis and delete any data which are no longer required in connection with the purpose for which they were originally obtained. When carrying out this exercise you should consider any legal or other requirements to retain data. You should also consider the type of relationship which Sypro Management Ltd. Limited has with the data subject and whether there is an expectation that we will retain data for any given period of time (eg our employees would expect us to retain their data for a period of time after they had left).

Sixth principle
Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

The rights which are referred to in the sixth principle are the data subject's rights in relation to:

18. access to his personal data;
19. preventing processing likely to cause damage or distress;
20. preventing processing for the purposes of direct marketing;
21. automatic decision-taking; If you receive a request in writing from an individual mentioning any of the above rights, you must pass that request promptly to the Data Protection Officer or Gerard Toplass as there are strict timescales within which we must respond.

Seventh principle
Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The seventh principle requires Sypro Management Ltd. Limited to take technical and organisational measures to protect personal data which we process:

22. technical measures include: software controls to restrict user access; up-to- date virus checking software; audit trail software; and encryption--all of which we have in place and manage through our

Data Protection Policy Guidance Note

IT department;

23. organisational measures include: restricting access to buildings and computer rooms; ensuring secure disposal of information; and training staff on the care and handling of personal data --all of which you are responsible for complying with and applying to your daily routine.

he Act imposes upon Sypro Management Ltd. Limited additional obligations if we use third parties to process personal data on our behalf. Examples of these third parties might include our external payroll providers, the company that provides disaster recovery services or our security and gatehouse services. Some of these third parties may have access to, or need to process, personal data on our behalf. If so, they will be acting as our data processors and the Act requires us to:

24. put in place a contract in writing with each of our data processors under which they agree to act only on instructions from us;
25. include the right to audit our data processors to ascertain compliance with the data protection requirements of the processing contract; and
26. ensure that the data processor agrees to comply with obligations equivalent to those imposed on us by the seventh principle.

If you are responsible for the selection, appointment or use of data processors, you must ensure that you only select those processors that are able to provide us with sufficient guarantees in respect of the technical and organisational measures they will apply to the processing of our personal data. Furthermore, if you are responsible for the drafting or negotiation of contracts with data processors, you must ensure those contracts contain all applicable data protection provisions. Seek further advice from the Data Protection Officer or our legal advisers Hamers Solicitors LLP.

The requirements of the seventh principle are set out in more detail in the Data Security Policy.

Eighth principle

Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

You must not transfer any personal data to any country outside the European Economic Area ('EEA'), unless you are authorised to do so. The EEA comprises the EU Member States plus Iceland, Norway and Liechtenstein. If you need to transfer personal data to a country outside the EEA you must consult with the Data Protection Officer or Gerard Toplass who will advise you further on how to comply with the adequacy requirements of the eighth principle.

Data subject rights

The sixth data protection principle requires us to comply with the rights of data subjects. It is important for you to familiarise yourself with these rights so that you may be able to identify them more easily. Each one is described below.

Right of subject access

Data subjects have a right of access to their personal data. A request for access will usually include a request for specific or general information relating to the applicant. If we receive such a request we must provide a description of:

27. the personal data relating to that data subject
28. the purposes for which the data are being processed
29. the recipients of the data
30. the information constituting the personal data
31. the source of those data (if available).

The Act lays down timescales within which we

Data Protection Policy Guidance Note

must comply with a request and requirements regarding how the information must be supplied. If you are authorised to handle subject access requests, you should follow the rules and procedures set out in the Subject Access Request Policy. If you are not authorised to handle such requests, you should not attempt to do so, but should forward the request to the Data Protection Officer or Human Resources Department.

Right to prevent processing likely to cause damage or distress Data subjects have the right to ask us not to process their personal data if:

32. the processing of those data in a particular way or for a particular purpose is causing, or is likely to cause, substantial damage or substantial distress to that data subject or another person; and
33. that damage or distress is, or would be, unwarranted.

You can usually identify a request to exercise this right because it will ask us to stop processing personal information about the individual. The Act lays down timescales within which we must comply with such a request. If you receive a request to stop processing you must forward it promptly to the Data Protection Officer or Human Resources Department. You should not attempt to deal with a request on your own.

Right to prevent processing for the purposes of direct marketing Data subjects have the right to request that we stop processing their personal data for direct marketing purposes. This means we must stop sending direct marketing materials to anyone that objects. You can identify a request made under this right because it is likely to ask us to stop sending unwanted marketing materials, otherwise referred to as 'junk mail' or 'spam', or stop making marketing calls.

If you receive a request to exercise this right you should forward it promptly to the Data Protection Officer or Head of the Marketing Department who will take the appropriate action to ensure that the individual's details are suppressed on our marketing database and he or she is no longer contacted by us for marketing purposes.

Right to object to automated decision taking Data subjects have the right to object to automated decisions being taken about them in relation to important matters that significantly affect them (such as evaluating performance at work, creditworthiness, reliability or conduct). This right is complex and subject to certain conditions. You can identify a request made under this right because it is likely to mention automated decisions or decisions made by computer and may ask us to take that decision again manually (ie using an individual instead of a computer). If you receive a request from any person exercising their right to object to automated decisions being taken about them, you should forward that request promptly to the Data Protection Officer or Gerard Toplass. You should not try to handle the request yourself.

Additional data subject rights
In addition to the rights specifically referred to in the sixth principle, data subjects also have the following rights:

34. the right to ask the Information Commissioner to carry out an assessment as to whether or not Sypro Management Ltd. Limited's processing is in accordance with the Act. This means the data subject has the right to make a complaint to the Commissioner and ask him to investigate. The Commissioner is obliged to consider all such requests and this could result in an investigation of our processing activities;
35. the right to take legal action against Sypro Management Ltd. Gohsei (UK Limited in the courts and claim compensation for any damage (or damage and distress) the data subject has suffered as a result of a breach of the Act; and
36. the right to apply to court for an order to rectify, block, erase or destroy inaccurate personal data and any expression of opinion based on those inaccurate data.

Data Protection Policy Guidance Note

Consequences of non-compliance
If we are found to be in breach of the Act, the Information Commissioner may issue enforcement proceedings against us which could result in our being prevented from further using personal data, or be required to change our processing procedures, or have other conditions imposed upon us in respect of the processing of personal data. Enforcement action will usually have a cost and time implication for the business. However, more damaging might be any restrictions imposed upon us which prevent us from exploiting our databases commercially. Additionally, the associated publicity could make us appear as an organisation that does not respect the privacy rights of individuals.

Affected data subjects may also take legal action against us and claim compensation for any breaches of the Act on our part that have resulted in damage (or damage and distress) to the data subject.

In certain circumstances, a negligent or deliberate breach of the Act could result in criminal liability not just for Sypro Management Ltd. Limited but for our employees also. For these reasons it is essential to comply with the provisions of the Data Protection Policy and this Guidance.
Contacts and responsibilities
If you have any queries regarding the Data Protection Policy, this Guidance or compliance with the Act in general, please contact the Data Protection Officer or Gerard Toplass for further advice.

The Data Protection Policy and this Guidance will be updated from time to time by the Data Protection Officer or Gerard Toplass to reflect any changes in legislation or in our methods or practices.

Policy For Handling Subject Access Requests

Introduction

Under the Data Protection Act 1998 ('Act'), individuals (such as employees, customers and business contacts) (collectively 'data subjects') have a general right of access to personal data which Sypro Management Ltd. Limited processes about them.

This Guidance is aimed at those members of staff who are authorised to handle access requests received by Sypro Management Ltd. Limited. If you are not one of these authorised members of staff, you should refer any request you receive to the Data Protection Officer or Human Resources Department.

Any failure to comply with this guidance may be a disciplinary offence which could result in summary dismissal. Negligent or deliberate breaches could result in criminal liability for you personally.

Handling subject access requests

1. Identifying a request 1.1 A request for access (referred to as a 'subject access request') is a request from a data subject to be given access to personal data which we process about him or her. For example, a letter which states 'please provide me with a copy of all the information that you have about me' will be a subject access request even though it does not expressly refer to personal data or to the Data Protection Act 1998.

1.2 All requests for access should be immediately directed to an authorised member of staff, which include the Data Protection Officer, the Compliance Officer and the Human Resources team. There are limited timescales within which we must respond to a request and any delay could result in our failing to meet those timescales, which could lead to enforcement action by the Information Commissioner and/or legal action by the affected individual.

2. Requirements for a valid request

2.1 For a subject access request to be valid, it must satisfy the following requirements:

2.1.1 the request must be in writing. If a data subject makes a request by telephone or in person, he or she should be asked to put that request in writing using the applicable Subject Access Request Form (as set out in Annexes 2 and 3 of this Guidance).

2.1.2 the request must be accompanied by the appropriate fee. We currently charge £10.

2.1.3 we must be able to identify the data subject making the request and then verify that identity. The Subject Access Request Form contains examples of the type of documents that can be used to do this. Typically we will request a copy of the data subject's driving licence or passport to enable us to establish his or her identity and signature (which should be compared to the signature on the Subject Access Request Form). We also ask for a recent utility bill (or equivalent) to verify the data subject's identity and address.

2.1.4 we must be able to identify the information being requested. For example, a subject access request may be made by someone who is both an employee and a customer. We can ask him or her to specify whether he or she is seeking access to his or her human resources file, customer records or both. The Subject Access Request Form contains questions designed to identify the information being requested and should be used wherever possible.

2.1.5 If the data subject makes a request that does not satisfy the above requirements you should write to him or her using the standard form letter set out in Annex 4 and enclosing the relevant Subject Access Request Form.

Data Security Policy

2.2 Unless the above requirements are met, we are not obliged to comply with a subject access request. However, we are obliged to notify the individual promptly if the fee is missing or if we require any information in order to fulfil the request.

3. Time period for satisfying a request

3.1 Once a valid subject access request is received, we have 40 days in which to respond. This 40-day period does not start to run until all these requirements have been satisfied. You should make a note of when this period commences.

4. Information to be provided in response to a request

4.1 The data subject is entitled to receive a description of the following:

4.1.2 the personal data we process about him or her;

4.1.3 the purposes for which we process the data;

4.1.4 the recipients to whom we may disclose the data;

4.1.5 the information constituting his or her personal data;

4.1.6 any information available regarding the source of the data;

4.1.7 the logic behind any automated decision we have taken about him or her (see below).

4.2 The above information must be provided in an intelligible form and any technical terms, abbreviations or codes must be explained to him or her. You should use the standard form letter in Annex 5 when providing the results of a subject access request.

5. Information about the logic behind automated decisions

5.1 If we are specifically asked in a subject access request for information about the logic behind any automated decision that we have taken in relation to important matters relating to the data subject (eg his or her performance at work, his or her creditworthiness, his or her reliability or conduct), we must provide a description of the logic involved in that automated decision, subject to the following conditions: the automated decision must have constituted the sole basis for the decision. For example, an application for credit which is conducted without any human intervention, other than to complete the application form, could be a decision which is taken solely by automatic means. However, if there is any element of human discretion as to whether or not to grant the credit, the decision would cease to be wholly automated and the data subject would not be entitled to a description of the logic.

5.2 In providing a description of the logic we are not required to reveal any information which constitutes a trade secret (e.g. the algorithm behind a credit scoring system).

6 How to locate information

6.2 The personal data we need to provide in response to a subject access request may be located in several of our electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

6.3 Depending on the type of information requested, you may need to search all or some of the following:

6.3.1 electronic systems (eg databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV);

6.3.2 manual filing systems (eg human resources filing system)--but only where the manual filing system falls within the definition of a ‘relevant filing system’--see paragraph 6;

Policy For Handling Subject Access Requests

6.3.3 data systems held externally by our data processors (specify, e.g. external payroll service providers);

6.3.4 occupational health records held by the Occupational Health Department;

7. What is a 'relevant filing system'?

7.1 The previous paragraph referred to a 'relevant filing system' as one of the systems that must be searched. A 'relevant filing system' is the name given to those manual filing systems that are subject to the Act because of the way they are structured internally and externally. To be a relevant filing system, the system must be:

7.1.1 a set of information relating to individuals- -the word 'set' suggests that there should be more than one file in the system or that there is a group of information by reference to a common theme. The files do not have to be located in the same geographical area to form a set but could be dispersed over different locations within the organisation;

7.1.2 structured by reference to individuals (such as a name, or employee or account number) or by reference to criteria relating to individuals (such as type of job, credit history, location) so that the filing system clearly indicates at the outset of any search whether specific information capable of amounting to personal data of the data subject is held within the system and, if so, in which file or files it is held;

7.1.3 structured in such a way that specific information relating to a particular individual is readily accessible (ie the system must have, as part of its structure or referencing mechanism, a sufficiently sophisticated and detailed means of easily indicating whether and where in an individual file specific criteria or information about the data subject can be readily located).

7.2 Therefore, a manual filing system which is subject to the Act must have an external and internal structure which allows specific personal data about an individual to be easily located without having to conduct a manual search of the entire file. If you have to thumb through the file to find specific information, the file is not a relevant filing system.

8. Information to be supplied in response to a request

8.1 Once you have carried out the search and gathered the results, you will need to select the information to be supplied in response to the subject access request. The data subject is only entitled to receive information which constitutes his or her personal data.

8.2 The type of information that will be classified as personal data is any information which:

8.2.1 identifies the data subject (either directly from the data or from those data and other information which is in our possession or likely to come into our possession [such as information held by other companies, offices and branches;

8.2.2 is biographical in a significant sense (eg it is more than a recording of the data subject's involvement in a matter or event that has no personal connotations, such as his or her attendance at a business meeting where his or her name appears in the list of attendees);

8.2.3 has the data subject as its focus (eg the information relates to the data subject personally rather than to some other person with whom he or she may have been involved or some transaction or event in which he or she may have figured);

8.2.4 affects the data subject's privacy, whether in his or her personal, or family life, business or professional capacity;

8.2.5 is an expression of opinion about the data subject;

8.2.6 is an indication of the intentions of Sypro Management Ltd. Limited or any other person towards the data subject (eg promotion prospects or redundancies).

Policy For Handling Subject Access Requests

8.3 Information about companies or other legal entities is not personal data. However, information about sole traders or partnerships will be, as the individuals within them are data subjects. Personal data relating to deceased persons are not covered.

8.4 The right of access is subject to a number of conditions and exemptions, particularly where the personal data reveal information about another individual--these are covered in paragraphs 8 and 11 below.

9. Examples of information likely to constitute personal data:

9.1 marketing lists containing a name together with contact details (eg address, telephone number, email);

9.2 customer profile information (e.g. purchasing patterns of the data subject);

9.3 Human resources information (e.g. salary details, appraisals);

9.4 financial information (e.g. information about the data subject's tax liabilities, income, expenditure);

9.5 medical information (e.g. medical history or condition, including pregnancy);

9.6 images caught on CCTV camera;

10. Examples of information that are unlikely to constitute personal data:

10.1 the reference to the data subject's name in a document that contains no other personal data about that data subject (e.g. the inclusion of the data subject's name in a list of attendees in the minutes of a meeting where the individual simply attended in his or her official capacity);

10.2 where the data subject's name appears in an email that has been sent to or copied to him or her, but where the content is not about him or her (e.g. emails sent to the data subject about Sypro Management Ltd. Limited's business dealings);

10.3 information about the performance of a department or branch office.

11. Disclosing personal data relating to other individuals

11.1 This paragraph sets out what you should do when the data subject's personal data includes information that identifies another person (e.g. as a source or recipient of the data subject's personal data).

11.2 You should first consider whether the other person's information constitutes personal data relating to the data subject. If this is not the case, then we are not obliged to provide that information. The other person's data should be blanked out so that he or she is not identified.

11.3 Where the other person's information does form part of the data subject's personal data, then you should consider:

11.3.1 whether the other person has consented to the disclosure of his or her information, or

11.3.2 whether it is reasonable in all the circumstances to comply with the request without the consent of the other person (e.g. because consent has been withheld or cannot be obtained, or because asking for consent might reveal the identity of the data subject).

11.4 In order to determine whether it is reasonable in all the circumstances to grant access, you should consider the following:

11.4.1 any duty of confidentiality that we owe to the other person;

11.4.2 any steps we have taken to obtain the consent of the other individual;

11.4.3 whether the other individual is capable of giving consent; and

11.4.4 any express refusal of consent by the other individual.

Policy For Handling Subject Access Requests

11.5 The following additional factors should also be considered:

11.5.1 whether the other person is a recipient or one of a class of recipients who might act on the data to the data subject's disadvantage;

11.5.2 whether the other person is the source of the information;

11.5.3 whether the information is generally known by the data subject; and

11.5.4 whether the data subject has a legitimate interest in the disclosure of the other person's information which he or she has made known to us.

11.6 Ultimately, whether or not it is reasonable to disclose the other person's information will depend upon all the circumstances and each request must be considered on a case-by-case basis.

11.7 If the decision is taken to withhold the other personal information, we still have an obligation to provide as much of the information requested as we can without disclosing the identity of the other person. This can usually be achieved by redacting the data (eg blanking out names or other identifying particulars). Always keep a record of what you have decided to do and your reasons for doing it.

12 How should the information be provided

12.1 The data subject is entitled to be provided with a copy of his or her personal data in a permanent form unless this is not possible, or would involve a disproportionate effort, or the data subject agrees otherwise.

12.2 In determining whether the provision of the data in permanent form is a disproportionate effort you should consider the following:

12.2.1 the cost of providing the information;

12.2.2 the time it will take to do so;

12.2.3 how difficult it may be for us to provide it;

12.2.4 the resources available within the organisation compared to the effort required.

12.3 These factors have to be balanced against the significance of the information to the data subject and any negative effect it will have on him or her if we do not provide it in permanent form.

12.4 If we cannot provide the data in permanent form, we must consider alternative ways of enabling the data subject to have access to the data. For example, we could invite him or her to our offices and allow him or her to view his or her data on screen, perhaps taking copies of the data that are of most interest to him or her (if this is possible), or where the data are CCTV images or telephone recordings, we can invite him or her to listen or view these onsite. If we allow the data subject to view his or her data on our premises, we need to ensure he or she is supervised and does not have access to confidential information or the personal data of others.

12.5 In all other cases, we should aim to provide the information in hard-copy form, redacted where appropriate.

13. Requests made by third parties on behalf of the data subject

13.1 Occasionally we may receive a request for subject access by a third party (an 'agent') acting on behalf of a data subject. These agents may include parents, guardians, legal representatives and those acting under a power of attorney or other legal authority. The agent must provide sufficient evidence that he or she is authorised to act on behalf of the data subject. The Subject Access Request Form in Annex 3 should be used for all such requests.

13.2 There are special rules for subject access requests regarding mentally and physically incapacitated adults. If the request you have received relates to an individual within either of these categories

Policy For Handling Subject Access Requests

specific advice should be sought from the Data Protection Officer or Human Resources Department or Compliance Officer.

14. Special rules regarding: mentally and physically incapacitated adults

14.1 An agent may also make a subject access request on behalf of a mentally or physically incapacitated adult who is incapable of making his or her own decisions or incapable of making a subject access request himself or herself. In this case, you should obtain from the agent either (i) a copy of his or her enduring power of attorney showing that he or she has been appointed to act as the data subject's agent, or (ii) evidence that he or she has been appointed by the Court of Protection to manage the property and affairs of the data subject.

15. Exemptions to the right of subject access

15.1 In certain circumstances we may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

16. Crime detection and prevention

16.1 We do not have to disclose any personal data which we are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. We are still required to provide as much of the personal data as we able to.

17. Confidential references

17.1 We do not have to disclose any confidential references that we have given to third parties for the purpose of actual or prospective:

17.1.1 education, training or employment of the data subject,

17.1.2 appointment of the data subject to any office; or

17.1.3 provision by the data subject of any service.

17.2 The exemption does not apply to confidential references that we receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual, which means you must consider the rules regarding disclosure of third party data set out in paragraph 8 before disclosing the reference.

18. Legal professional privilege

18.1 We do not have to disclose any personal data which are subject to legal professional privilege. There are two types of legal professional privilege:

18.1.1 Advice privilege: this covers confidential communications between Sypro Management Ltd. Limited and our lawyers where the dominant purpose of the communication is the giving or receiving of legal advice;

18.1.2 Litigation privilege: this covers confidential communications between Sypro Management Ltd. Limited or its lawyers and a third party (such as a witness) where the dominant purpose of the communication is the giving or seeking of legal advice in respect of current or potential legal proceedings. The claim to legal professional privilege in litigation ends as soon as the case has been decided and, at that moment, the documents in the file which were subject to legal professional privilege become available if a subject access request is received.

19. Management forecasting

19.1 We do not have to disclose any personal data which we process for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity. Examples of management forecasting and planning activities include staff relocations, redundancies,

Amended GDPR Privacy Policy 25th May 2018

Background

Sypro Management Limited understands that your privacy is important to you and that you care about how your personal data is used. We respect and value the privacy of everyone who visits this website, www.sypro.co.uk, and any associated websites or portals used to access any of our software solutions and services ("Our Site"), or any information, data supplied relating to projects, contracts or any commercial arrangements [in email, PDF, excel, hard or soft copy] ("Customer Data") and as described in Parts 5 and 6, below, we do not collect personal data about you unless you contact us. Any personal data we do collect will only be used as permitted by law.

Please read this Privacy Policy carefully and ensure that you understand it. Your acceptance of this Privacy Policy is deemed to occur upon your first use of Our Site, or submission of Customer Data. If you do not accept and agree with this Privacy Policy, you must stop using Our Site immediately, or, request any Customer Data to be destroyed.

1 Information about us

Our Site is owned and operated by Sypro Management Limited, a limited company registered in England under company number 06413057. Registered address: 19 Bowlalley Lane, Hull, England, HU1 1XR. Main trading address: 19 Bowlalley Lane, Hull, England, HU1 1XR. VAT number: 923 5505 35. Data Protection Officer: N/A As defined by the ICO regulations. We can confirm that GDPR is a standing point on every board meeting agenda, and the directors consider GDPR as part of the normal day to day running of the business.

2. What does this policy cover?

This Privacy Policy applies only to your use of Our Site and your supply of Customer Data. Our Site may contain links to other websites. Please note that we have no control over how your data is collected, stored, or used by other websites and we advise you to check the privacy policies of any such websites before providing any data to them.

3. What is Personal Data?

Personal data is defined by the General Data Protection Regulation (EU Regulation 2016/679) (the "GDPR") as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier'. Personal data is, in simpler terms, any information about you that enables you to be identified. Personal data covers obvious information such as your name and contact details, but it also covers less obvious information such as identification numbers, electronic location data, and other online identifiers.

4. What Are My Rights?

Under the GDPR, you have the following rights, which we will always work to uphold:

a) The right to be informed about our collection and use of your personal data. This Privacy Policy should tell you everything you need to know, but you can always contact us to find out more or to ask any questions using the details in Part 10.

b) The right to access the personal data we hold about you. Part 9 will tell you how to do this.

c) The right to have your personal data rectified if any of your personal data held by us is inaccurate or incomplete. Please contact us using the details in Part 10 to find out more.

d) The right to be forgotten, i.e. the right to ask us to delete or otherwise dispose of any of your personal data that we have. Please contact us using the details in Part 10 to find out more. We store limited personal data about users that have/ had access to our software solutions and services, and timescales for storing such data is governed by the contract between Sypro Management Limited and its customer. It is a requirement to store contract data for several years, to assist in defect management and historical records, and these timescales can be changed where the customer requests, and the contract is varied.

e) The right to restrict (i.e. prevent) the processing of your personal data.

f) The right to object to us using your personal data for a particular purpose or purposes.

g) The right to data portability. This means that, if you have provided personal data to us directly, we are using it with your consent or for the performance of a contract, and that data is processed using automated means, you can ask us for a copy of that personal data to re-use with another service or business in many cases.

h) Rights relating to automated decision-making and profiling. We do not use your personal data in this way.

For more information about our use of your personal data or exercising your rights as outlined above, please contact us using the details provided in Part 10. Further information about your rights can also be obtained from the Information Commissioner's Office or your local Citizens Advice Bureau. If you have any cause for complaint about our use of your personal data, you have the right to lodge a complaint with the Information Commissioner's Office.

5. What Personal Data Do You Collect?

Subject to the following, we do not collect any personal data from you. We do store temporary cookies in order to confirm your identity when accessing the site. We do not use any other means of data collection.

If you send us an email, we may collect your name, your email address, and any other information which you choose to give us.
Any member of staff will provide additional personal data to allow for payroll to be processed and to ensure we are compliant with our HMRC and other requirements.

6. How Do You Use My Personal Data?

If we do collect any personal data, it will be processed and stored securely, for no longer than is necessary in light of the reason(s) for which it was first collected. We will comply with our obligations and safeguard your rights under the GDPR at all times. For more details on security see Part 7, below.

As stated above, we do not generally collect any personal data. If you contact us and we obtain your personal details from your email, we may use them to respond to your email.

Any and all emails (which may contain your personal data), are retained as part of an audit trail to support contract and commercial agreements and variations, and helpdesk and issue resolutions for service and support. You have the right to withdraw your consent to us using your personal

any time, and to request that we delete it.

We will not share any of your data with any third parties for any purposes other than storage on an email server. For any staff members, data may be shared with external agencies including payroll bureaus, government agencies and approved third parties. Where there is a requirement to share data at a personal request, this authorisation will be documented.

7. How and where do you store my data?

We will only store your personal data in the UK. This means that it will be fully protected under the GDPR.

Please contact us using the details below in Part 10 for further information about the particular data protection mechanism used by us when transferring your personal data to a third country. Personal data security is essential to us, and to protect personal data, we take the following measures:

7.1 All internal business applications (Outlook, Excel, OneDrive etc.) are installed locally and where installed externally, are secured using standard login credentials and password.

7.2 All hosted platforms (AWS, UKFast, etc.) are only accessibly by authorised members of staff using a minimum of login credentials and password, and where appropriate, two factor authentication.

7.3 We do not store any staff member personal data in hard copy, and any Customer Data may be worked on via hard copy, but will be destroyed immediately after completion.

8. Do You Share My Personal Data?

We will not share any of your personal data with any third parties for any purposes, subject to the following exception, and the reasons detailed in part 6 above.

In some limited circumstances, we may be legally required to share certain personal data, which might include yours, if we are involved in legal proceedings or complying with legal obligations, a court order, or the instructions of a government authority.

9. How Can I Access My Personal Data?

If you want to know what personal data we have about you, you can ask us for details of that personal data and for a copy of it (where any such personal data is held). This is known as a “subject access request”.
All subject access requests should be made in writing and sent to the email or postal addresses shown in Part 10.
There is not normally any charge for a subject access request. If your request is ‘manifestly unfounded or excessive’ (for example, if you make repetitive requests) a fee may be charged to cover our administrative costs in responding. We will respond to your subject access request within 10 working days and, in any case, not more than one month of receiving it. Normally, we aim to provide a complete response, including a copy of your personal data within that time. In some cases, however, particularly if your request is more complex, more time may be required up to a maximum of three months from the date we receive your request. You will be kept fully


Sypro