
DATA PROTECTION POLICY

Contents	Page
1. Introduction	2
2. Scope	2
3. Objectives	2
4. Application of the Policy & Employees' Responsibility	2
5. ICO Notification & Assessment	3
6. Obtaining & Processing Data	3
7. Data Accuracy	3
8. Subject Rights & Access Requests	3
9. Information Security	4
10. Managing Employee Data	5
⇒ Recruitment	5
⇒ Equal Opportunities Monitoring	6
⇒ References	6
⇒ Basic Employee Details	6
⇒ Payroll Information	6
⇒ Appraisal Records	7
⇒ Disciplinary & Grievance Records	7
⇒ Drug & Alcohol Testing	7
⇒ Company E-mails	7
11. Company Website	8
12. CCTV Monitoring	8
13. Useful Links	8
Appendix 1: Glossary of Terms	9
Appendix 2: DPA 1998 – The 8 Principles	10
Appendix 3: Sensitive Data	11

1. Introduction

SGS United Kingdom Ltd (hereafter “the Company”) is committed to protecting the rights of individuals’ privacy with regard to the processing of personal data. It has established the following policy to support this commitment.

The Company regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between employees and those with whom it carries out business. The Company will ensure that it treats personal information lawfully and correctly and seeks to fully endorse and adhere to the principles established in the Data Protection Act 1998 (hereafter “the Act”).

2. Scope

This policy covers the processing of personal data (i.e. information about living individuals) whose use is controlled by the Company and defined in the Company’s Data Protection Notification. It applies to any employees or agents of the Company who process personal data on behalf of the Company. Personal data applies to both computer and manual records, including filing systems and audio-visual records.

This policy does not apply to processing undertaken by individuals for private ends, even in cases where Company equipment is used for such processing. However, the Company does continue to require adherence to the principles of this data protection policy by associated or partner institutions in any case where data is shared between the Company and other organisations.

3. Objectives

The Company seeks to ensure that all processing of personal data carried out on its behalf will comply with the requirements of the Act, including the eight principles of good practice laid out in Schedule 1 of the Act (listed in Appendix 2). To these ends, the Company seeks in particular to ensure that all those processing data on their behalf are aware of their obligations in processing data under the Act and that data subjects are made aware of their rights, which must be respected by the Company.

4. Application of the Policy & Employees’ Responsibility

All current employees of the Company, whether permanent, casual, temporary or fixed term, implicitly consent to the processing of personal data relating to them necessary for the performance of the employee’s contract and/or to conduct the Company’s business.

Employees are required at all times during their employment to comply with the provisions of the Act and with any associated policies introduced by the Company. Appropriate disciplinary action, possibly leading to dismissal, will be taken in cases where an individual has committed a clear and wilful breach of the Act’s requirements. Employees are further informed that any breach of the Act may represent a criminal offence for which they are personally liable.

The Company’s Data Controller (currently the UK HR Manager) has overall responsibility for data protection matters, reviewing the policy and for maintaining the Company’s Notification with the Information Commissioner. Furthermore, the Data Controller will report to senior management on issues of importance relating to the Act, provide advice on matters arising and co-ordinate responses to Subject Access Requests.

Line managers have a responsibility to ensure that all relevant employees are fully informed of their responsibilities under the Act and have access to this policy.

Finally, it is the responsibility of the IT Services Manager to ensure the security of all data held on the Company's computer systems.

5. ICO Notification & Assessment

The Company undertakes to maintain an accurate and timely notification of its data processing activities with the Information Commissioner's Office (ICO), which shall be available on request to data subjects. Maintenance of the notification is the responsibility of the Company's Data Controller. Employees must be made aware that, in cases where they undertake new processing, they must inform the Data Controller so that the Company notification can be reviewed.

The Company reserves the right to audit data processing being undertaken in any of its constituent departments, to ensure that processing is legitimate and that the Company notification remains valid.

The Company will co-operate with any Data Protection assessment instigated by the ICO and employees will be expected to assist with any assessment.

6. Obtaining & Processing Data

In line with the requirements of Principle 1 of the Act (*fair and lawful processing*), the Company seeks to ensure that whenever a 'data subject' submits information, they are clearly informed about the uses of that information (a fair processing notice) and, where relevant, they give their informed consent for processing.

These requirements will be enforced whatever the means of collection (whether paper forms, email, surface mail correspondence, web data collection forms, or any other medium). Where practicable, all collection media should carry clear statements regarding likely processing.

Sensitive data shall only be collected for certain specified purposes, and shall be obtained with consent. The Company will keep the collection and processing of sensitive data to a minimum, and will only process sensitive data for the purposes described in Appendix 3.

7. Data Accuracy

In line with the requirements of Principle 4 of the Act, the Company seeks to ensure that all personal data held is accurate and timely. Data will be reviewed periodically and, where practical and appropriate, the Company will provide subjects with copies of data holdings so that inaccurate or out-of-date information may be identified and eradicated, or updated. Data subjects have a responsibility to ensure that they inform the Company of any changes to their details.

8. Subject Rights & Access Requests

The Company undertakes to honour the rights of all data subjects as laid out in the Act and will respond in good time to any Subject Access Request, as long as the enquirer has submitted the appropriate fee (a £10 fee may be charged at management discretion).

The Company seeks to ensure that no data processing undertaken will cause unwarranted damage or distress to data subjects and will correct or erase, as appropriate, any data that is found to be incorrect.

Mechanism for Subject Access Requests

The Company undertakes to co-operate as fully as is reasonable with any Subject Access Request. However, the Company reserves the right to refuse to comply with repetitious subject access requests where a reasonable time has not elapsed between the previous and current request.

All Subject Access Requests must be routed via the Company's Data Controller and should be made in writing. Once initiated, a standard search for data will be conducted against a pre-defined set of likely data-holders. However, subjects will be permitted, additionally, to specify any other potential data-holders whose records should be searched. In the event that the requested data is not supplied (e.g. when this would challenge the data protection rights of some other third party) then the enquirer will be informed in writing of the reasons for the non-disclosure.

Responses to Subject Access Requests will be provided within 28 days and in a permanent form, unless it is believed that this would involve disproportionate effort or the data subject agrees otherwise. Any codes shown shall be translated or explained to the data subject.

9. Information Security

The Company is committed to holding data in secure conditions, and will make every effort to safeguard against accidental loss and corruption of data. All employees have a responsibility to keep data securely. Appropriate measures must be taken to ensure that there is no unauthorised access to areas in which records are held. Storage areas that are unattended should be locked, as should relevant offices, where practicable.

Personal files should be kept away from the public gaze and, where possible, employees should operate a 'clear desk' policy. When manual records are no longer required they should be disposed of securely via the Company's 'confidential waste' arrangement.

All computer 'personal record' systems should be backed up regularly to ensure against loss of data, and PCs should be virus-protected. Access to records systems will be by password only and employees may not share passwords or login as some other user. Passwords should be changed on a regular basis.

Access to any centrally maintained records system can be authorised only by the relevant systems administrator. Visual Display Units should not be visible to unauthorised people, and should be guarded with password-protected screen-savers where possible. When PCs are recycled for use elsewhere or taken out of service, they should ideally be degaussed or have their hard drives overwritten to US Department of Defence standards before reuse or disposal. This is particularly pertinent if the PCs concerned have been used to process personal and /or sensitive data (e.g. data processed by members of the HR or Finance teams).

Any employee who processes personal data on a laptop that they use beyond the confines of Company premises will be responsible for the safe keeping of that data and that equipment. If travelling, the laptop should be kept in view, or secured in locked luggage. All departments must seek to ensure that employee information is not placed accidentally in the public domain.

Dealing with third party enquiries

The Company is committed to data security, and will make every effort to safeguard against illegitimate disclosure of personal information. Internal data transfers made between different departments of the Company should be made on an operational basis only.

Disclosures to third parties shall be made only where at least one of the 'conditions for fair processing' (Principle 1) have been met, as follows:-

- ⇒ the subject's consent has been obtained;
- ⇒ or disclosure is necessary in relation to a contract to which the subject is a party;
- ⇒ or disclosure is in compliance with a legal obligation placed on the Company;
- ⇒ or disclosure is necessary to protect the subject's vital interests;
- ⇒ or disclosure is necessary for the purposes of legitimate interests pursued by the Company.

Similarly, where sensitive data is to be disclosed at least one of the following conditions will need to be met:-

- ⇒ the subject's explicit consent has been obtained;
- ⇒ or disclosure answers a legal obligation in connection with employment;
- ⇒ or disclosure is necessary to protect the subject's vital interests;
- ⇒ or the information disclosed as already been put in the public domain by the actions of the data subject;
- ⇒ or disclosure is in relation to any legal proceedings;
- ⇒ or disclosure is in connection with the monitoring of equality of opportunity.

Where an ad-hoc request for personal information is received from a third party, the identity of that third party and the need for the information must be established before disclosure is even considered. External disclosure of employee data should be made only by the Human Resources Department. Disclosure to the Police may be made by the Company in cases where the Police are pursuing a criminal investigation. In all cases, if there is any doubt as to the validity of the enquirer or their enquiry, no disclosure should be made and advice should be sought from a senior manager or the Company's Data Controller.

10. Managing Employee Data

Recruitment (General) – All recruitment activity carried out by the Company, or appointed agencies, should comply with the provisions of the Act. In accordance with the third principle of the Act, the Company will not collect 'excessive' data concerning individuals that has no relevance to the recruitment process (e.g. asking for copies of a driving licence for a desk-based position). All job applications will be treated as confidential and should not be distributed to persons other than those directly involved in the recruitment process. Similarly, to ensure security of data, all information collected during a recruitment campaign should be returned to the central Human Resources department for safe storage. Records will be kept for a period of six months, unless candidates have been informed that their details will be retained for a longer period and for reasons that can be justified (e.g. holding a pool of talented candidates for potential future vacancies).

Equal Opportunities Monitoring – In accordance with the Company's Equality & Diversity policy, personal data is processed by the Company for the purposes of equal opportunities monitoring. As this information is potentially of a sensitive nature, access to data is restricted to the individual concerned and members of the Human Resources team who are

responsible for analysing equal opportunities initiatives. During the recruitment process, equal opportunities monitoring forms are used to collect data on each applicant, but these will remain anonymous and isolated from the selection exercise.

References – References issued on behalf of the Company should largely comprise brief statements of fact and minimal opinion. Where opinion is given, it should be supported with factual evidence wherever possible. All employees shall be made aware that references they write may become available to the subject in certain circumstances. Under no circumstances should 'sensitive data', such as details of health or criminal convictions, be included in a reference unless there is legal reason for such data.

N.B. – Managers are strongly recommended not to give references themselves and to refer any requests to the central Human Resources team at Ellesmere Port.

References received by the Company may be made available to the subject on request. All standard reference request forms should make this clear to the referee, and all departments should ensure that referees are fully aware of the possibility of subject access. In the event that such a request is received, the advice of the Company's Data Controller should be sought, who will normally seek the consent of the provider of the reference, or consider whether the provider would suffer any harm if the information was disclosed without consent, before proceeding.

Basic Employee Details – Basic records kept by the Company will typically include such things as name, address, communication details, date-of-birth, emergency contacts and bank details. All are covered by the Act as they are recorded on the Company's HR Information System. In order to comply with a number of requirements of the Act (data security, accuracy, relevance, etc) employee details should be stored in a limited number of secure locations and the content held should be for legitimate reasons.

The Company engages a finite number of third party organisations to who personal data is disclosed (e.g. pension providers, out-sourced payroll, etc) and this information is available from the Data Controller. Similarly, certain statutory requirements will involve the permissible disclosure of personal data to government bodies such as HMRC, CSA, HSE, etc.

Payroll Information – Various components of an individual's pay amount to personal data under the Act, including basic pay, bonuses, benefits and allowances that are held on the Company's HR Information Systems. The Company, as data controller, is also responsible for ensuring third party payroll processing agents are compliant with the Act, ensuring compliance in particular with the Act's seventh principle - data security.

Whilst salary information regarding an individual may not technically amount to sensitive personal data, it is recognised that pay is a sensitive issue for many employees. The Company's pay banding structure discloses certain broad information for large parts of the workforce and it is accepted that, in the interests of transparency, a level of knowledge can be ascertained regarding pay ranges for different jobs or grades. However, individual rates of pay remain a confidential matter between the employee and the Company and such information will be processed in accordance with the first principle of the Act.

Appraisal Records – The Company's Performance Management policy requires that each employee receives an annual performance review. Typically, appraisal meetings are documented on standard forms which are sent via email and recorded on HR systems. As such, the records are generally covered by the Act and should contain information that is

relevant, not misleading and used only in the context of informing or supporting decisions related to employment.

Managers should ensure that subjective opinions are avoided where possible, or at least supported by facts. Personal information offered by an employee that a manager chooses to record to explain performance issues (e.g. if an individual had been going through a divorce) will be classed as sensitive data. In such circumstances, it is important that the employee completes their section of the appraisal record to indicate consent has been given to process the information.

Disciplinary & Grievance Records – Documents generated during a disciplinary or grievance investigation that are scanned or entered onto the HR Information System will be covered by the Act. Hard copies that are not held in a structured filing system will not.

Complainants or witnesses involved in the process should be informed that the individual may see the evidence against them and that confidentiality cannot be guaranteed. However, the Company will not disclose third party data in certain circumstances, e.g. if it is felt that the third party may suffer harm as a result of the disclosure.

The Company will not normally retain disciplinary documents relating to allegations that were not proven following an investigation and hearing. Whilst not used further within a disciplinary context, details of warnings that have ‘expired’ for disciplinary purposes will not be removed from records. The Company considers it appropriate to be aware of the full history of an employee’s career and may use this information to inform other employment-related decisions.

Drug & Alcohol Testing – The Company can require employees to undergo drug or alcohol tests as a part of the employment contract when there are grounds to suspect they are intoxicated, or on a random basis. Such testing is seen as fair and lawful for large parts of the workforce where there are clear health and safety reasons for conducting tests. The processing of resultant data will be covered by the Act if recorded electronically or sent via email and should not be excessive and should serve an immediate and definite purpose.

Records will only be retained if there is a compelling reason to do so, e.g. for safety reasons or on-going disciplinary investigations. Otherwise, all records should be promptly destroyed.

Company E-mails – Personal data contained in any emails (whether outgoing or incoming) are covered under the Act because they are created and held on computer systems. Personal data includes any expression of intention or opinion about an individual and all employees should guard against such communications via email unless they are justified and based on fact. As a guide, employees should refer to the Group’s published ‘Email Etiquette’ document in order to comply with the provisions of the Act whilst using this particular medium.

The Company may access email accounts in the course of managing its business (e.g. to ensure customers queries are picked up in somebody’s absence) or if there is a need to monitor activity as part of an investigation based on a reasonable suspicion that individuals are sending or receiving inappropriate emails. To ensure the Company focuses on a *need* to monitor as opposed to an *ability* to monitor, any such investigations will need prior approval of senior Group management. Please refer to the Company’s IT User and Internet Policy for more information.

11. Company Website(s)

The Company maintains a strong web presence which may contain basic personal details of certain employees for commercial reasons. Such information will normally be restricted to include their name, business contact details, professional qualification, relevant experience/competence, etc.

Additional personal information may be posted on the Web (e.g. in the form of a CV), but will not be displayed without the explicit consent of the individuals involved (this includes images of employees who appear on promotional photographs, etc).

12. CCTV Monitoring

The Company operates CCTV monitoring systems in a number of its locations, essentially to assist in the detection and deterrence of crime. Such systems will be operated in such a way as to safeguard individuals' right to privacy and images obtained will be treated as personal data and managed according to the principles of the Act (as detailed in the linked CCTV Code of Practice published by the ICO) and this policy. All sites should highlight the existence of CCTV cameras with appropriate signage.

All CCTV images have ownership and copyright vested in Company. Consent to use or reproduce material held by the Company resulting from the CCTV system will normally be withheld. Data on tapes will normally be preserved for one month. After this period, if they are not needed for evidential purposes, the tapes will be re-used. If required for evidential purposes, they will be retained for as long as is necessary to the prosecution of the case.

Individuals may request in writing to see a tape they believe may hold images of them and this will be treated in the same ways as all other subject access requests.

13. Useful Links

ICO – Employment Practices Code

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/index.html

ICO – Employment Practices Code (Supplementary Guidance)

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practice_code_-_supplementary_guidance.pdf

ICO – Quick Guide to Employment Practices Code

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/quick_guide_to_employment_practices_code.pdf

ICO – CCTV Code of Practice

http://www.ico.gov.uk/upload/documents/cctv_code_of_practice_html/index.html

Appendix 1: Glossary of terms

Data controller: A person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

Data processor: A person, who processes personal information on a data controller's behalf. Anyone responsible for the disposal of confidential waste is also included under this definition.

Data subject: This is the living individual who is the subject of the personal information (data).

Enforcement notice: The Information Commissioner has the power to serve an enforcement notice if he is satisfied that a data controller has contravened or is contravening the data protection principles. The notice must set out the steps that the data controller must take to comply with the relevant requirements of the Act. The notice may be appealed to the Information Tribunal which may confirm, amend or overturn it. However, in the absence of an appeal, if the data controller fails to comply with a notice, a criminal offence is committed.

Notification: Notification is the process by which a data controller's processing details are added to a register. Under the Data Protection Act every data controller who is processing personal information needs to notify unless they are exempt. Failure to notify is a criminal offence. Even if a data controller is exempt from notification, they must still comply with the data protection principles. The Commissioner maintains a public register of data controllers available at www.ico.gov.uk. A register entry only shows what a data controller has told the Commissioner about the type of data being processed. It does not name the people about whom information is held.

Personal data: Personal data means information about a living individual who can be identified from that information and other information which is in, or likely to come into, the data controller's possession.

Processing: Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.

Relevant filing system: Any filing system that is structured with reference to individuals (or criteria relating to individuals).

Subject access request: Under the Data Protection Act, individuals can ask to see the information about themselves that is held on computer and in some paper records. If an individual wants to exercise this subject access right, they should write to the person or organisation that they believe is processing the data.

Appendix 2: The Eight Principles

Principle 1: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one [appropriate] condition is met.

Relevant conditions for processing data:

- ⇒ The data subject has given consent;
- ⇒ Processing is necessary for the performance of a contract to which the data subject is a party;
- ⇒ Processing is necessary for compliance with any legal obligation placed on the controller;
- ⇒ Processing is necessary to protect the vital interests of the data subject;
- ⇒ Processing is necessary for the purposes of legitimate interests pursued by the data controller, or by third parties to whom the data is disclosed (except where this might prejudice the rights or freedoms of the data subject).

Relevant conditions for processing *sensitive* data:

- ⇒ The data subject has given explicit consent;
- ⇒ Processing is necessary for compliance with any legal obligation placed on the controller that relates to employment;
- ⇒ Processing is necessary to protect the vital interests of the data subject;
- ⇒ The information involved has already been made public by the subject;
- ⇒ Processing is necessary for the purposes of / in connection with legal proceedings;
- ⇒ Processing is necessary for reviewing equality of opportunity.

Principle 2: Personal data shall be obtained for one or more specified and lawful purposes and shall not be processed in any manner incompatible with those purposes.

Principle 3: Personal data shall be adequate, relevant and not excessive to the purposes for which they are processed.

Principle 4: Personal data shall be accurate and, where necessary, up to date.

Principle 5: Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

Principle 6: Personal data shall be processed in accordance with the rights of data subjects under the Act.

Principle 7: Appropriate measures shall be taken against unauthorised processing of personal data and accidental loss or destruction of personal data.

Principle 8: Personal data shall not be transferred to a country outside the EEA unless,

- ⇒ The data subject has given consent;
- ⇒ Transfer is necessary for the performance of a contract to which the data subject is a party;
- ⇒ Transfer is made for reasons for substantial public interest;
- ⇒ Transfer is necessary to protect the vital interests of the data subject;
- ⇒ Transfer is necessary for the purposes of, or in connection with, legal proceedings.

Appendix 3: Sensitive Data

The Act defines sensitive data as data relating to:

- ⇒ Ethnic origin;
- ⇒ Political opinion;
- ⇒ Religious beliefs;
- ⇒ Trade Union membership;
- ⇒ Physical and mental health;
- ⇒ Sexual life;
- ⇒ Criminal record.

The Company undertakes to process sensitive data only where relevant conditions apply. Employees are advised not to collect sensitive data unless there is proven need for this information. The circumstances in which the Company accepts that sensitive data will have to be processed will include the following:-

- ⇒ Compilation of relevant monitoring data for government agencies (e.g. for the Equality Commission in Northern Ireland);
- ⇒ Recruitment to positions with financial responsibility or with access to potentially vulnerable persons (in relation to criminal record information);
- ⇒ Recording sensitive information for the purpose of any legal proceedings;
- ⇒ Collection of data that is necessary for medical purposes;
- ⇒ Data that is processed in relation to racial or ethnic origin, used for genuine ethnic monitoring to safeguard the rights and freedoms of data subjects.

If employees wish to process data for reasons other than those given above, they should contact the Company's Data Controller for advice before commencing processing.