| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.1.1 Categories of Personal Data** | | | |
| a) What type of personal data do you process?<br>Please give examples of any sensitive data that you process. | | | |
| b) (i) Are sensitive personal data differentiated from other personal data?<br>(ii) If so, how? | | | |
| c) If not, why not? | | | |
| c) (i) Are sensitive personal data processed differently to other personal Data Protection within the organisation?<br>(ii) If so, how? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.1.2 Schedule 2 - Grounds for Legitimate Processing of Personal Data** | | | |
| a) Have you identified all the categories of personal data which you are processing and how?<br>If so, can you list them: | | | |
| b) Have you identified the purposes for which you are processing personal data and how?<br>If so, can you list them: | | | |
| c) Have you identified which of the grounds in Schedule 2 you will be relying on as providing a legitimate basis for processing personal data?<br>If so, can you list them:<br>(Show interviewee text of Schedule 2). | | | |
| d) (i) Will you be relying on different grounds for different categories of personal data?<br>(ii) If so, how was this assessment made? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.1.3 Schedule 3 - Grounds for Legitimate Processing of Sensitive Personal Data** | | | |
| a) Have you identified the categories of *sensitive personal data* that you are processing? If so, how?<br>If so, can you list them: | | | |
| b) Have you identified *the purposes* for which you are processing sensitive personal data? If so, how?<br>If so, can you list them: | | | |
| c) Have you identified which of the grounds in Schedule 3 you will be relying on as providing a legitimate basis for processing sensitive personal data?<br>If so, can you list them:<br>(Show interviewee text of Schedule 3/Orders under Sch 3 (10)). | | | |
| d) (i) Will you be relying on different grounds for different categories of sensitive personal data?<br>(ii) If so, how was this assessment made? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.1.4 Obtaining consent** | | | |
| a) If you are relying on the individual providing consent to the processing as grounds for satisfying Schedule 2, when and how is that consent obtained? | | | |
| b) If you are relying on the individual providing explicit consent to the processing as grounds for satisfying Schedule 3, when and how is that consent obtained? | | | |
| | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.1.5 Lawful Processing** | | | |
| *If you are a public sector organisation:*<br>a) (Does your processing of personal data fall within your statutory powers? If so what are they and how are they identified? | | | |
| b) Has compliance with the Human Rights Act been assessed? | | | |
| *All organisations:*<br>c) Do you assess whether any of the personal data that you process is held under a duty of confidentiality? | | | |
| d) If so, how is that assessment made? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.1.5 Lawful Processing (continued)** | | | |
| e) How is that confidentiality maintained? (e.g. Instructions on disclosure or shredding) | | | |
| f) Do you assess whether your processing is subject to any other legal or regulatory duties? | | | |
| g) If so, how is that assessment made? | | | |
| h) How do you ensure that those legal duties are complied with? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.1.6 Fair Processing** | | | |
| a) How are individuals made aware of the identity of your organisation as the data controller? | | | |
| b) When are individuals made aware of the identity of your organisation as the data controller? | | | |
| c) How are individuals made aware of how their personal data will be used? | | | |
| d) When are individuals made aware of these uses? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.1.6 Fair Processing (continued)** | | | |
| e) How are individuals offered the opportunity to restrict processing for other purposes? | | | |
| f) When is that opportunity offered? | | | |
| g) (i) Is any other information offered to the individual regarding your organisation's processing?<br>(ii) If so, which information? | | | |
| h) (i) How is that information provided to the individual?<br>(ii) And when? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.1.6 Fair Processing (continued)** | | | |
| h) Do you receive information about individuals from third parties? (Please give examples) If yes, go to Question J, if not go to G.1.7. | | | |
| i) (i) If you do receive information about individuals from third parties, how are individuals informed that the data controller is holding personal data about them?<br>(ii) And if so, when? | | | |
| | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.1.7 Exemptions from the First Data Protection Principle** | | | |
| The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:-<br>1. the identity of the data controller<br>2. the identify of any nominated data protection representative, where one has been appointed<br>3. the purpose(s) for which the data are intended to be processed<br>4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair | | | |
| a) (i) Do you provide individuals with all of this information?<br>(ii) Is this always the case? (If yes, go to Section G.2.1)<br>If your organisation does not provide this information to data subjects, which exemption to these provisions is being relied upon? | | | |
| b) How is that exemption identified? | | | |
| c) How is correct reliance on the exemption assessed? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.2.1 Uses of Personal Data within the organisation** | | | |
| a) What are the procedures for maintaining a comprehensive and up-to-date record of use of personal data? | | | |
| b) How often is this record checked? | | | |
| c) Does the record include all equipment which can process personal data and data held in relevant filing systems? | | | |
| d) Does the record cover processing carried out on your behalf (e.g. by a Data Processing Bureau)? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.2.2 Notifying the Data Subject** | | | |
| a) What is the procedure for notifying (where necessary) the data subject of the purpose for processing their personal data?<br>(Cross reference with section G.1.6 of the First Principle) | | | |
| **G.2.3 Notification to the Commissioner** | | | |
| See Annex H, section H.2 | | | |
| **G.2.4 Use of Existing Personal Data for new purposes** | | | |
| a) How is the use of existing personal data for new purposes communicated to:-<br>• the data subject,<br>• the person responsible for Notification within the organisation, and<br>• the Information Commissioner?<br>b) What checks are made to ensure that further processing is not incompatible with its original purpose? ` | | | |
| **G.2.5 Notification Maintenance** | | | |
| See Annex H, section H.2 | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.2.6 Disclosures of Data** | | | |
| a) Is there a departmental/organisational policy on disclosures of data within your organisation/to third parties? | | | |
| b) Has it been documented? | | | |
| c) How are staff made aware of this policy/instructed to make disclosures? | | | |
| d) How are individuals/data subjects made aware of disclosures of their personal data? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.2.6 Disclosures of Data (continued)** | | | |
| e) Do you assess the compatibility of a 3rd party's use of the personal data to be disclosed? (If no, go to Section G.3.1) | | | |
| f) If so, how do you make the assessment? | | | |
| | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.3.1 Adequacy and relevance of Personal Data** | | | |
| a) Why are you holding the personal data? | | | |
| b) How is the *adequacy* of personal data for each purpose determined? (Please give examples.) | | | |
| c) How is an assessment made as to the *relevance* (i.e. no more than the minimum required) of personal data for the purpose for which it is collected? | | | |
| d) (i) What are the procedures for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?<br>(ii) How often are these procedures reviewed? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.3.1 Adequacy and relevance of Personal Data (continued)** | | | |
| e) Do you have any procedures for assessing the amount and type of personal data collected for a particular purpose? If so, what are they? | | | |
| f) Are items of personal data held in every case when they are only relevant to some? | | | |
| g) If staff are allowed to enter free text, what guidance is given to ensure its relevance? | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.4.1 Accuracy of Personal Data** | | | |
| a) Are personal data evaluated to establish the degree of damage to both the data subject/data controller that could be caused through inaccuracy? | | | |
| b) How, and how often, are personal data checked for accuracy? Please give examples: | | | |
| c) In which circumstances is the accuracy of the personal data checked with the Data Subject? Please give examples: | | | |
| d) (i) Is the accuracy of personal data assessed at the time of collection from sources other than the data subject to whom the data relates?<br>(ii) If so, how? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.4.1 Accuracy of Personal Data (continued)** | | | |
| e) (i) Are the sources of personal data (i.e. Data Subject, Data User, or third party) identified in the record?<br>(ii) If so, how? Please give examples.<br>(iii) Is there any facility to record notifications received from the data subject that they believe their data to be inaccurate? | | | |
| | | | |
| | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.4.2 Keeping Personal Data Up-to-Date** | | | |
| a) Are personal data evaluated to establish the degree of damage to:<br>• the data subject or<br>• data controller<br>that could be caused through being out of date? | | | |
| b) Are there procedures to determine when and how often personal data requires updating? | | | |
| c) Are there procedures to monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals?<br>(Cross-reference with Section G.3.1on the Third Principle). | | | |
| d) (i) Are data duplicated and held separately at different locations by different departments?<br>(ii) If so, how are updates/amendments communicated to all parties with copies of the data? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.4.2 Keeping Personal Data Up-to-Date (continued)** | | | |
| e) How are third parties to whom the data has been disclosed, informed of any amendments to the personal data? (This is best practice). | | | |
| f) How are complaints about inaccuracies dealt with? | | | |
| | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.5.1 Retention Policy** | | | |
| a) (i) What are the criteria for determining the retention periods of personal data?<br>(ii) And how often are these criteria reviewed? | | | |
| b) Have the retention periods been implemented and adhered to in practice? | | | |
| c) (i) Is a record kept of the dates on which relevant personal data were created and/or obtained?<br>(ii) Do systems include the facility to set retention periods? If so has the facility been used? | | | |
| d) Are there any statutory requirements on retention? If so, please give examples. | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.5.1 Retention Policy (continued)** | | | |
| e) Are there any sector standards on retention? If so, please give examples. | | | |
| | | | |
| | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.5.2 Review and Deletion of Personal Data** | | | |
| a) (i) Is there a review policy?<br>(ii) If so, has it been documented? | | | |
| b) When it is no longer necessary to retain data which was collected for a particular purpose<br>• How is a review made of the data to determine whether it should be deleted?<br>• How often is the review conducted?<br>• Whose is responsible for determining the review?<br>• If the personal data are held on a computer, does the application include a facility to flag records for review/deletion? | | | |
| c) Are personal data reviewed at intervals to determine if:<br>• retention in an archive is necessary or<br>• they can be retained in an anonomised format (e.g. if kept only for historical or statistical purposes)? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.5.2 Review and Deletion of Personal Data (continued)** | | | |
| d) Are there any exceptional circumstances for retaining certain data for longer than the normal period? | | | |
| e) What are they? | | | |
| f) Who makes that assessment? (Name and Job title) | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.5.3 Deletion of Personal Data** | | | |
| a) What guidance is provided on deleting personal data no longer relevant when the purpose for processing ceases to exist? | | | |
| b) (i) What is your policy on how personal data are deleted/destroyed? (e.g. shredding)<br>(ii) Is this different for sensitive personal data? | | | |
| Cross Reference with the Seventh Principle Annex G, Section G.4, Destruction of Personal Data. | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.1 Subject Access** | | | |
| a) How does the organisation identify subject access requests that are received from individuals? | | | |
| b) (i) How does the organisation identify the individual making the request? | | | |
| c) (i) Does the organisation request information from the individual in order to locate the information requested?<br>(ii) If so, how? | | | |
| d) How do you locate all personal data relevant to a request (including any appropriate 'accessible records')? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.1 Subject Access (continued)** | | | |
| e) On receipt of a request, does your organisation continue to carry out routine processing of the personal data relevant to the request? | | | |
| f) If this involves amending or deleting information relevant to the request, how is this managed in relation to the individual? | | | |
| g) How is the response collated? | | | |
| h) How is the information provided to the individual? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.1 Subject Access (continued)** | | | |
| i) How is the individual provided with the relevant information about your organisation's/departments' processing? | | | |
| j) Is the individual provided with a copy of the information held? | | | |
| k) If the individual consents to *only* seeing the information, how is that arranged? | | | |
| h) (i) If any of the response is not in plain language, does the organisation provide an explanation of any codes or other unintelligible information?<br>(ii) If so, how? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.1 Subject Access (continued)** | | | |
| m) Is information relating to or identifying third parties identified in the information to be provided? | | | |
| n) If third party information is identified, is it provided to the individual making the request? | | | |
| o) If not, on what grounds would the information about third parties be withheld? | | | |
| p) How does your organisation ensure that the response is provided within the statutory timeframe? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.2 Withholding of personal data in response to a subject access request** | | | |
| a) (i) Are there any circumstances where your organisation would withhold personal data from a subject access request?<br>(ii) If so, how are the grounds for doing so, identified? | | | |
| b) (i) Do you rely on a subject access exemption? (if no, then go to Section G.6.3.)<br>(ii) If so, how is that exemption identified? | | | |
| c) (i) Is correct reliance on the exemption assessed?<br>(ii) If so, how and by whom? | | | |
| d) If your organisation does not rely on an exemption to the subject access provisions, which provision of the Act does it rely upon to withhold subject access? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.3 Processing that may cause Damage or Distress** | | | |
| a) Are there any procedures for reviewing the processing of personal data before it begins? | | | |
| b) Would the review include an assessment of how to avoid causing damage or distress to an individual? | | | |
| c) Do you take into account the possibility that damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court? | | | |
| d) Do you take any steps to alert staff of possible compensation claims? Please give examples: | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.3 Processing that may cause Damage or Distress** | | | |
| e) (i) Are you aware of any processing currently underway that may cause damage or distress to an individual?<br>(ii) If so, what is it? | | | |
| f) What are the procedures, if any, for responding to a data subject notice/Court Order asking you as the Data Controller to cease or not the begin processing of personal? | | | |
| g) Do the procedures take account of the need to respond to a notice within 21 days? | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.4 Right to Object** | | | |
| a) What is the procedure for complying with an individual's request to prevent processing for the purposes of direct marketing or for any other reason? | | | |
| b) Are direct marketing files checked against marketing suppression lists such as the Mailing Preference, Fax and Telephone Preference Services? | | | |
| | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.5 Automated Decision Taking** | | | |
| a) Are there any decisions made affecting individuals that are based solely on processing by automatic means? | | | |
| b) If so, what is the procedure(s) for notifying an individual that an automated decision-making process has been used? | | | |
| c) What are the procedures for responding within 21 days to a data subject notice that this decision be reconsidered or be taken via other means? | | | |
| d) Do the procedures identify 'exempt decisions' (s.12 DPA)? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.6 Rectification, blocking, erasure and destruction** | | | |
| a) What is the procedure for responding to a data subject's notice (in respect of accessible records) or a court order requiring:<br>• rectification,<br>• blocking,<br>• erasure or<br>destruction of personal data? | | | |
| b) What is the procedure for notifying third parties to whom the data has been disclosed of the results of a data subject's request for rectification, blocking, erasure or destruction of personal data? | | | |
| | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.6.7 Staff Awareness** | | | |
| a) How are staff instructed to recognise and respond to initial subject access requests? | | | |
| b) How are staff instructed to respond to a formal data subject notice? | | | |
| Cross reference with the Data Protection Policy, Annex F.1.3, Staff Awareness and Training | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.7.1 Security Policy** | | | |
| a) Is there a Data Security Policy? (This must be shown to the Auditor.) | | | |
| b) If so, who/which department(s) is responsible for drafting and enforcing the Data Security Policy within the organisation? | | | |
| c) How are the potential harm to the data subject and the nature of the data assessed to decide if the policy is appropriate? | | | |
| d) Is the level of security set taking in to account the state of technological development in security products and the cost of deploying these? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.7.1 Security Policy (continued)** | | | |
| e) (i) How often is the Data Security Policy reviewed?<br>(ii) What are the procedures for doing so? | | | |
| f) Does the Data Security Policy specifically address data protection issues? | | | |
| g) (i) Do you adhere to BS7799 or any other security standards/codes of practice?<br>(ii) If so, which one(s)? | | | |
| h) What are the procedures for monitoring compliance with the Data Security Policy within the organisation? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.7.1 Security Policy (continued)** | | | |
| i) How often is compliance with the Data Security Policy assessed and by whom/which department? | | | |
| j) (i) Are there any procedures for managing non-compliance?<br>(ii) If so, what are they? | | | |
| k) (i) Does the Data Security Policy apply to the organisation as a whole?<br>(ii) If not, then to which departments does it not apply and why? | | | |
| l) (i) Are there any additional security policies/procedures being adhered to by individuals or departments which are not part of the overall organisational Data Security Policy?<br>(ii) If so which individuals/departments and why? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.7.2 Unauthorised or unlawful processing of data** | | | |
| a) (i) Does your security policy clearly identify what constitutes unlawful and unauthorised processing?<br>(ii) If so, please tell me. If not, can you give examples. | | | |
| b) Which security measures are in place to prevent any unauthorised or unlawful processing of:<br>• Data held in an automated format (e.g. password controlled access to PCs)<br>• Held in a manual record (e.g. locked filing cabinets)? | | | |
| c) (i) Is there a higher degree of security to protect *sensitive* personal data from unauthorised or unlawful processing?<br>(ii) If so, what are the procedures? | | | |
| d) What procedures are in place to detect breaches of security (remote, physical or logical)? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.7.3 Reliability of Staff** | | | |
| a) Have staff processing personal data been made aware of the Security Policy?<br>Cross reference with the Data Protection Policy, Annex F.1.3, Staff Awareness and Training. | | | |
| b) (i) Are staff given any security and risk management training?<br>(ii) If so, what does the training involve? | | | |
| c) How often are staff given training on how to implement security procedures? (Write in departments to which the reply refers.) | | | |
| d) Is training documented in guidelines/staff handbook for future reference? Please give examples: | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.7.3 Reliability of Staff (continued)** | | | |
| e) How is access to personal data restricted to authorised staff? e.g. on a need to know basis | | | |
| f) Is each department responsible for controlling access to its personal data, or is this task centralised? | | | |
| g) How is access to systems and locations restricted to authorised personnel? | | | |
| h) (i) Are staff authorised to take equipment/software for external use/to work from home (eg a laptop)?<br>(ii) If so, do they receive any specific instructions on how personal data, which may be stored on this equipment/software, should be safeguarded? Please give examples: | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.7.4 Destruction of Personal Data** | | | |
| a) How is the destruction of personal data that are no longer necessary carried out to prevent unauthorised access? | | | |
| b) Are there different procedures for destroying *sensitive* personal data? | | | |
| Cross Reference with the Fifth Data Protection Principle, Annex G.5.3, Deletion of Personal Data. | | | |
| | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.7.5 Contingency Planning - Accidental loss, destruction, damage to personal data** | | | |
| a) Is there a contingency plan to manage the effect(s) of an unforeseen event? | | | |
| b) (i) If so, has this plan been tested? How often?<br>(ii) Has the contingency plan been amended as a result of the test? If so, how? | | | |
| c) (i) Are staff informed of contingency procedures?<br>(ii) If so, how often? | | | |
| d) (i) Are personal data backed-up? If so how often? e.g. on site/off site<br>(ii) Where are the back ups held? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.7.5 Contingency Planning - Accidental loss, destruction, damage to personal data (continued)** | | | |
| e) (i) Do you permit live data to be used for testing purposes?<br>(ii) If so, what procedures are used to protect the personal data during and after testing? | | | |
| f) What are the risk management procedures, if any, to recover data (both automated and manual) which may be damaged/lost through:<br>• human error<br>• computer virus<br>• network failure<br>• theft<br>• fire<br>• flood<br>• other disaster? | | | |
| **G.7.6 Contracts for Processing Carried out by Third Parties** | | | |
| Please refer to Annex H, Section H.1. | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.8.1 Adequate Levels of Protection** | | | |
| a) Are you aware of the issues surrounding this Principle? | | | |
| b) (i) Does the organisation transfer personal data to a country or territory outside the EEA?<br>(ii) If so, where? (If no, do not ask any other questions on this Principle.) | | | |
| c) What are the purposes for making transfers of personal data abroad? | | | |
| d) What are the types of data transferred? (e.g. contact details, employee records) | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.8.1 Adequate Levels of Protection (continued)** | | | |
| e) Are any sensitive personal data transferred abroad? If so, please provide details. | | | |
| f) What are the main risks involved in the transfer of personal data to countries outside the EEA? | | | |
| g) What measures are taken to ensure an adequate level of security when the data are transferred to another country or territory? | | | |
| h) Has the organisation checked whether the non EEA state has been deemed as having adequate protection? | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation

| Question/Check | Evidence (Documents) Examined | Findings and Observations | Result |
|---|---|---|---|
| **G.8.2 Exempt Transfers** | | | |
| a) Does the organisation carry out any transfers of data where it has been decided that the Eighth Principle does not apply? | | | |
| b) If so what are they? | | | |
| c) To which country/territory are these transfers made? | | | |
| d) What is the criteria set by your organisation, which must be satisfied before a decision is made about whether the transfer is exempt from the Eighth Principle? E.g. consent, (See Schedule 4, DPA 1998, for a full list) | | | |

**KEY:** COM = Complies MAJ = Major Non-compliance MIN = Minor Non-compliance OBS = Observation