IC	**G: Compliance Audit Checklists: The Eight Data Protection Principles**			**Page**	37
Organisation		**Department**		**Date**	
Aspect	**G.7 The Seventh Principle**	**Auditor**		**Audit ref:**	

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

IC	**G: Compliance Audit Checklists: The Eight Data Protection Principles**			**Page**	38
Organisation		**Department**		**Date**	
Aspect	**G.7 The Seventh Principle**	**Auditor**		**Audit ref:**	

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? (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? (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

IC	**G: Compliance Audit Checklists: The Eight Data Protection Principles**			**Page**	39
Organisation		**Department**		**Date**	
Aspect	**G.7 The Seventh Principle**	**Auditor**		**Audit ref:**	

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? (ii) If so, what are they?			
k) (i) Does the Data Security Policy apply to the organisation as a whole? (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? (ii) If so which individuals/departments and why?			

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

IC	**G: Compliance Audit Checklists: The Eight Data Protection Principles**			**Page**	40
Organisation		**Department**		**Date**	
Aspect	**G.7 The Seventh Principle**	**Auditor**		**Audit ref:**	

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? (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: • Data held in an automated format (e.g. password controlled access to PCs) • 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? (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

IC	**G: Compliance Audit Checklists: The Eight Data Protection Principles**			**Page**	41
Organisation		**Department**		**Date**	
Aspect	**G.7 The Seventh Principle**	**Auditor**		**Audit ref:**	

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? 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? (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

IC	**G: Compliance Audit Checklists: The Eight Data Protection Principles**			**Page**	42
Organisation		**Department**		**Date**	
Aspect	**G.7 The Seventh Principle**	**Auditor**		**Audit ref:**	

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)? (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

IC	**G: Compliance Audit Checklists: The Eight Data Protection Principles**			**Page**	43
Organisation		**Department**		**Date**	
Aspect	**G.7 The Seventh Principle**	**Auditor**		**Audit ref:**	

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

IC	**G: Compliance Audit Checklists: The Eight Data Protection Principles**			**Page**	44
Organisation		**Department**		**Date**	
Aspect	**G.7 The Seventh Principle**	**Auditor**		**Audit ref:**	

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? (ii) Has the contingency plan been amended as a result of the test? If so, how?			
c) (i) Are staff informed of contingency procedures? (ii) If so, how often?			
d) (i) Are personal data backed-up? If so how often? e.g. on site/off site (ii) Where are the back ups held?			

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

IC	**G: Compliance Audit Checklists: The Eight Data Protection Principles**			**Page**	45
Organisation		**Department**		**Date**	
Aspect	**G.7 The Seventh Principle**	**Auditor**		**Audit ref:**	

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? (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: • human error • computer virus • network failure • theft • fire • flood • 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