

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	26
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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? (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	

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	27
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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	

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	28
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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 <i>only</i> 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? (ii) If so, how?					
KEY:	COM = Complies	MAJ = Major Non-compliance	MIN = Minor Non-compliance	OBS = Observation	

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	29
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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	

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	30
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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? (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.) (ii) If so, how is that exemption identified?					
c) (i) Is correct reliance on the exemption assessed? (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	

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	31
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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	

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	32
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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? (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	

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	33
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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	

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	34
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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	

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	35
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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: <ul style="list-style-type: none"> • rectification, • blocking, • erasure or 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					

IC	G: Compliance Audit Checklists: The Eight Data Protection Principles			Page	36
Organisation		Department		Date	
Aspect	G.6 The Sixth Principle	Auditor		Audit ref:	
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	