Data Protection Act 1998

Monetary Penalty Notice

Dated: 20 August 2013

Name: Islington Borough Council

Address: Town Hall, Upper Street, London, N1 2UD

Introduction

1. This Monetary Penalty Notice is issued by the Information Commissioner ('the Commissioner') pursuant to section 55A of the Data Protection Act 1998 ('The Act'). A monetary penalty notice is a notice requiring the data controller to pay to the Commissioner a monetary penalty of an amount determined by the Commissioner and specified in the notice.

2. Islington Borough Council is the data controller, as defined in section 1(1) of the Act, in respect of the processing of personal data carried on by Islington Borough Council (referred to in this notice as 'the data controller').

3. Following a serious contravention of the data controller's duty, under section 4(4) of the Act, to comply with the seventh data protection principle, the Commissioner considers, for the reasons set out below, to serve on the data controller notice of a monetary penalty in the sum of £70,000.

Statutory framework

---

4. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is the data controller.

5. Under sections 55A and 55B of the Act (introduced by the Criminal Justice and Immigration Act 2008 which came into force on 6 April 2010) the Commissioner may, in certain circumstances, where there has there been a serious contravention of section 4(4) of the Act, serve a monetary penalty notice ('MPN') on a data controller requiring the data controller to pay a monetary penalty of an amount determined by

the Commissioner and specified in the notice but not exceeding £500,000.

6. The Commissioner has issued Statutory Guidance under section 55C (1) of the Act about the issuing of monetary penalties which is published on the Commissioner's website. It should be read in conjunction with the Data Protection (Monetary Penalties and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

7. This case involves the disclosure of sensitive personal data. Sensitive personal data is defined in section 2 of the Act (in so far as it is applicable to this case) as follows:-

"In this Act "sensitive personal data" means personal data consisting of information [in so far as applicable to the facts of this case] as to –

(a) the racial or ethnic origin of the data subject

(e) his physical or mental health or condition,

(f) his sexual life

(g) the commission or alleged commission by him of any offence…"

Power of Commissioner to impose a monetary penalty

8. Section 55A of the Act provides that:

(1) The Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that –

(a) there has been a serious contravention of section 4(4) [of the Act] *by the data controller,*

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller –

(a) knew or ought to have known –

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

Background

---

9. On 27 May 2012, a request was made to the data controller under the Freedom of Information Act 2000 ('FOIA') via a website called 'Whatdotheyknow' ('WDTK').

10. WDTK is a publicly accessible website which enables individuals and organisations to submit requests for information to public authorities. Requests under FOIA and responses to them are uploaded to the site and are available to all those wishing to view them. WDTK is well known in Information Governance circles. Indeed, prior to the response to this request, the data controller had responded to several requests via this site dating back to 1 April 2008. The data controller was therefore familiar with the use of WDTK when responding to requests.

11. The request and its response were handled by the data controller's Information Governance Officer ('IGO'). However, to provide a response to at least one of the questions, the IGO needed to obtain information from the data controller's Housing Performance Team as this team had access to the data controller's housing information system as well as the skills required to extract the information required in a suitable format.

12. The Housing Performance Team sent three excel workbooks with the information required ('the workbooks') via email to the IGO. The workbooks contained spreadsheets (or worksheets). However, the Housing Performance Team did not advise the IGO that additional data was also contained within the worksheets in the form of pivot tables. Pivot tables in Excel are a reporting tool that makes it easy to extract information from large tables of data without the use of formulas. A pivot table is used for sorting and summarizing the data in a worksheet or database file. It can automatically sort, count, and total spreadsheet data and then display the results in a second table showing the summarized data.

13. The IGO performed visual checks on the three workbooks, removing a personal tab attached to one of the workbooks, and was satisfied that no further personal data was visible. No further checks were therefore

carried out. However, the IGO was not familiar with pivot tables and was therefore unaware that there was data contained in a pivot table behind the worksheets. The Commissioner notes that the hidden spread sheets can be revealed by a user with basic knowledge of Excel

14. The IGO disclosed the data by email to WDTK on three separate occasions:-

i) 26 June 2012 at 09:05

ii) 26 June 2012 at 09:34

iii) 27 June 2012 at 13:23

First disclosure

15. On the first occasion on 26 June 2012 at 09:05, the Council responded to the request by sending the workbooks to the WDTK website. One workbook contained an open spread sheet, the other two workbooks contained personal data in four hidden spread sheets.

16. The Housing Performance Team was sent a copy of the FOI response and informed the IGO that personal data had not been removed from the Excel workbooks. At 09.22 the IGO then attempted to recall the

message through a facility within Microsoft Outlook and received confirmation that the recall had been successful.

17. However, it should be noted that WDTK cannot process such recall requests. An email recall in general is not considered a particularly robust method of ensuring containment in such incidents. Further, despite the inclusion of 'whatdotheyknow' in the email address to which the recall request was made, the IGO was under the incorrect impression that the email address was that of an individual and not of an organisation that would place the information on the internet.

Second disclosure

18. The IGO, having performed a visual check of the workbooks, again concluded that there was no personal data on the worksheets and sent the same FOI response again on 26 June at 9.34 am, 29 minutes after the initial disclosure was made. This email which had the three worksheets attached contained personal data, all of which this time was contained in hidden worksheets.

19. On 27 June 2012 at 8.21 am, the IGO sent an email to WDTK asking for the original message to be deleted, after the IGO had been advised by their IT department that a recall request through Microsoft Outlook

would not necessarily work to email recipients outside of the Islington network.

20. No attempt was made to call back the second email, since as far as it was known at the time, no personal data was included.

Third disclosure

21. At this point, the incident was compounded further when, on 27 June 2012 at 13:23, the IGO sent a replacement message to WDTK with the three workbooks attached. On this occasion, the personal data was again contained within the hidden sheets.

22. The pivot table summaries produced in each workbook by the Housing Performance Team should have been copied and pasted (with just the values and not the entire format) on to blank sheets to remove the hidden data sheets. The data analyst however failed to do this before sending the completed documents to the IGO. The IGO was not informed how this data was produced or what data lay behind the tables and lacked the necessary skills, support and guidance to proactively check this.

23. No formal request was sent by the data controller to WDTK or My Society (the host of WDTK) to officially take down the information. Therefore all correspondence with the attachments sent by the data controller remained publicly accessible on WDTK.

24. On 14 July 2012, a WDTK volunteer administrator, whilst reviewing success rates of requests, happened to read the exchanges and, upon seeing personal data on the first workbook, WDTK removed the record from public access. The volunteer did so by completing internal take down documentation and also filed a URL removal request to Google to get any copies of the request page and the spreadsheets removed from their cache. It is noted that WDTK and not the data controller acted to remove this information from its own site and from the Google cache.

25. Google responded to the request and confirmed the cached copies had been deleted apart from one copy of the cached request pages which was still being shown as pending.

26. Copies of the data remains on the MySociety servers but can only be accessed by individuals with WDTK administration rights.

27. WDTK has advised that during the period of time that the information was accessible there were ten download requests (excluding the WDTK

administrator). Three were from 'Microsoft Office Existence Discovery'. It is therefore likely that there were seven instances of individual files being downloaded.

28. On 16 July 2012 MySociety notified the ICO of the incident. The data controller was similarly made aware of the breach on 16 July 2012, when MySociety also emailed the data controller to notify the data controller of the breach. As the data controller was aware that MySociety had notified the ICO of the incident, the data controller was of the view that it therefore did not need at that stage to proactively report the matter itself.

29. The Commissioner understands from the data controller that the data controller was not aware of this breach until contacted by MySociety. Upon receipt of this email, the data controller confirmed that the breach had been contained by MySociety.

30. The Commissioner understands that the data controller then immediately began the process of analysing the data that had been breached, in order to identify the data subjects and their contact details, so they could be notified of the breach. The data controller simultaneously began an investigation into the circumstances of the breach.

31. On 26 July 2012, the data controller's data security manager ('DSM') called the ICO's helpline for a discussion on the case. The DSM was informed that the incident had been logged and assigned to a case worker to deal with. The data controller interpreted this as further confirmation that the ICO had been notified and therefore did not complete a self-reported breach notification form.

32. The three workbooks uploaded to WDTK in response to the request contained:-

    i) Workbook 1 – Placements though the data controller's Private Sector Opportunities Scheme over the 2 year period ending on 31 March 2012 (309 records)
    ii) Workbook 2 – Allocations of housing accommodation to new tenants over the 2 year period ending on 31 March 2012 (1330 records)
    iii) Workbook 3 – Allocations of housing accommodation to existing tenants over the 2 year period ending on 31 March 2012 (736 records).

33. The data hidden within the pivot tables in the three workbooks included the following personal data, much of which is "sensitive", relating to

2,375 individuals / families who had submitted applications for council housing or were themselves data controller's tenants:-

- Name
- Relationship status
- Gender / gender identity
- Ethnicity
- Religion
- Sexuality
- Assessment of priority housing need (includes the number of dependent children, whether victim of domestic violence, dyslexic, elderly, ex-offender, whether a mental health patient, medical / special needs, pregnant or a pensioner?
- Whether their household is overcrowded
- Whether they have local connections
- Who referred the application (council worker, social services, relative etc.)
- Deposit amount paid
- Placement (property address
- Incentive paid
- Name of agent / landlord
- Further notes on the application

34. A statistical breakdown below establishes the extent of sensitive data involved in the breach. Information which is most likely to give rise to substantial distress is marked in bold:-

Category	Number
Name of applicant[1]	2,204
Address of applicant (either placement or application address)	2,375
Gender	2,341
Sexuality	**140**
Ethnic Origin	**2,375**
Religion	**100**
Domestic Violence / Harassment	**21**
Ex Offender	**1**
FLOS (Floating support – usually given to care leavers)	78
Impairments noted	**2**
Med / Medical	**56**
MH / MHP / Mental Health	**7**
MOB (Mobility)	6
OVC (Overcrowding)	42

[1] This number is a reflection that some individuals made applications on behalf of a family who fulfil the total number of data subjects in the address category.

Pension / DLA / Elderly / OAP	5
Person's Age	171
RC (Reception Centre)	9
V (Violence)	**11**
WCH (Wheelchair)	6

Policies in relation to FOIA / disclosure of information

35. Whilst the data controller did have in place an 'Access to Information Policy' which nominates an IGO to lead on responding to FOIA requests and take responsibility for ensuring that the responses are made within the statutory frameworks, there are no consistent or standard 'safety checking mechanisms' across the data controller. Different checks exist in different departments. Some requests are 'historically reviewed' and some IGOs raise concerns with the Information Compliance Manager on a case by case basis.

36. In this case, apart from the visual checks undertaken by the IGO responsible to ascertain whether any personal data was obviously present, no safety checking mechanism was in place.

37. Whilst the data controller insists as a matter of internal policy that all IGOs remove any information that can be used to identify an individual from responses, in this case, since the IGO was not aware of any personal data and as no safety checking mechanisms were present, there was no sufficiently effective means of identifying personal data hidden in pivot tables.

38. Further, there is no documentation to establish confirmation / authorisation for the release of information by anyone other than the IGO. Effectively, this means that there was no peer review or additional quality assurance process in place.

39. The roles and responsibilities section of the Access to Information Policy appears to concentrate on the release of information rather than the need to consider the DPA aspects of sensitive disclosure.

Training

40. At the time of the contravention, there was no specific training or policy in place in relation to Excel. It is each manager's responsibility to ensure that role based training is provided and completed by staff, depending on the work they are required to perform. There was

however a lack of technical training / supervision and checking mechanisms.

41. Whilst the data controller has provided classroom based training to specific teams in departments that held and processed sensitive data to other departments, at the time of the contravention, the staff involved in the incident had not yet received this training.

42. Whilst the data controller's Access to Information Policy states that the IGO is the lead on responding to FOI requests and they take ultimate responsibility, the IGO in this case was not equipped with the skills and training to effectively deal with FOI requests and to recognise when personal data may have been placed at risk when provided in formats such as Excel.

Communication

43. The failure of the data analyst, who carried out the further statistical analysis on the Excel spreadsheets to convert it into a pivot table facility within the spreadsheets, to communicate this fact to the IGO is considered to be a further contributory factor.

Grounds on which the Commissioner proposes to serve a monetary penalty notice

---

44. In deciding to issue this Monetary Penalty Notice, the Commissioner has considered the facts of the case and the deliberations of those within his office who have recommended this course of action. In particular, he has considered whether the criteria for the imposition of a monetary penalty have been met; whether, given the particular circumstances of this case and the underlying objective in imposing a monetary penalty, the imposition of such a penalty is justified and whether the amount of the proposed penalty is proportionate.

Serious contravention of section 4(4) of the DPA

45. The Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act in that there has been a breach of the data controller's duty to comply with the Seventh Data Protection Principle.

46. The Seventh Data Protection Principle provides, at Part I of Schedule 1 to the Act, that:

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

47. Paragraph 9 at Part II of Schedule 1 to the Act further provides that:

"Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to –

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected"

48. The Commissioner considers that the contravention in this case is serious for the following reasons:-

i) Sensitive personal data has been placed online and made available on a global scale including data concerning sexuality, ethnicity, domestic violence and criminal offending.

ii) 2,375 data subjects were affected of which a substantial proportion had sensitive personal data disclosed as a result of the breach.

iii) There were no sufficient technical or organisational measures in place to prevent the data controller contravening the seventh data protection principle. In particular:-

a) Whilst the data controller had dedicated IGOs in post, there was no formal or consistent process in place for checking an FOI response.

b) There were no specific checking procedures built into that process to check whether personal or sensitive personal data was present ahead of providing a response to an FOI request.

c) There were no sufficient procedures in place to train staff to carry out such checks and as such the data controller failed to equip its staff with the appropriate knowledge and skills.

The contravention is of a kind likely to cause substantial damage or substantial distress

49. The Commissioner is further satisfied that the contravention in this particular case is of a kind likely to cause substantial damage or substantial distress for the following reasons:-

i) Confidential personal data was disclosed to unauthorised third parties (via the internet) due to the inappropriate technical and organisational measures taken by the data controller.

ii) The data in this case is highly sensitive. The statistical breakdown clarifies the extent of sensitivity marked against the number of data subjects. The total number of data subjects affected is 2,375.

iii) During the period of time that the data was accessible to the public (18 days) there were 10 download requests (excluding the WDTK administrator). It is likely that there were 7 instances of individual files being down loaded.

iv) The data subjects would suffer from substantial distress knowing that their confidential personal data has been disclosed to third parties (via the internet) and that there is the possibility that their data may have been further disseminated and possibly misused. That is so, even if those concerns do not actually materialise in practice.

v) The affected individuals had entrusted their detailed information to the data controller, on the basis that it would be dealt with in confidence.

vi) If the data has been disclosed to untrustworthy third parties then it is likely that the contravention would cause further distress and

also substantial damage to the data subjects such as exposing them to identity fraud and possible financial loss.

The data controller ought to have known that there was a risk that the contravention would occur, that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but failed to reasonable steps to prevent the contravention

50. The Commissioner is satisfied that section 55A (3) of the Act applies in that the data controller ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but it failed to take reasonable steps to prevent the contravention.

51. The Commissioner is satisfied that the data controller ought to have known that there was a risk that the contravention would occur for the following reasons:-

i) Whilst the data controller's IGO was routinely responsible for dealing with FOI requests, she was nevertheless not equipped with the knowledge, guidance and information governance tools to check the accuracy and content of the information before being sent out.

ii) Due to a lack of a robust checking policy, the IGO failed to query or check the information before sending it out on more than one occasion.

52. Further, the data controller ought to have known that there was a risk that such a contravention would be of a kind likely to cause substantial damage or substantial distress for the following reasons:-

i) The workbooks released contain sensitive personal data with the potential to cause those affected substantial damage or substantial distress. In particular, the presence of information on sexuality, ethnicity, mental health and domestic violence has the potential to cause distress.

ii) The information related to 2,375 data subjects.

iii) The data controller should have known that the information would be available to multiple people once it had been loaded on to the website.

iv) The data controller should have known that if information was disclosed in error this would be available to the public via the WDTK website as the request came through the WDTK website and it was not just responding to the requester.

53. Finally, the data controller failed to take reasonable steps to prevent the contravention as follows:-

i) An effective training programme for staff had not been implemented. The person responsible for disclosing the information had not been trained properly to enable them to identify sensitive personal data contained in the pivot tables nor had they received any specific data protection training. They were therefore unable to mitigate against the risk of an unlawful disclosure.

ii) Whilst the data controller had some standard procedures in place for dealing with FOI requests, the data controller did not have appropriate technical or organisational measures in place to firstly screen and check whether personal data was present in information being prepared for disclosure and secondly to check it, prior to it being disclosed in response to an FOI request.

iii) There is no documented procedure that specified that a request must be checked by a peer.

iv) The data controller's initial containment of the incident was poor and the error was repeated a second and third time, providing further evidence of their inadequate and weak procedures to minimise risk.

v) Once the IGO was informed that personal information was contained in the first response to the request, the IGO did not seek further assistance or return to the source data to extract only that which was actually needed. This opportunity provided sufficient time to try and contain the matter but appropriate and swift action was not taken.

54. In the circumstances, the data controller knew, or ought to have known that there was a risk that these contraventions would occur, and would continue to occur, unless reasonable steps were taken to prevent the contravention such as those suggested above.

Aggravating features the Commissioner has taken into account in determining the amount of a monetary penalty

Effect of the contravention

55. The fact that the disclosure was in response to an FOI request and would be available to the public at large, supported by the fact that the information was available for 18 days and was subject to numerous accesses.

56. The data controller had the opportunity to put the breach right but failed adequately to act on information received from the website.

57. The breach was repeated a second and third time (supporting the view that both the initial controls and any remedial measures which may otherwise have prevented further incidents were lacking).

58. There was a general lack of urgency to report the breach to the ICO regardless of the ICO being informed by MySociety.

59. The data controller informed the affected data subjects on 24 July 2012, 10 days after the incident was reported to the ICO and 28 days after the initial incident.

Mitigating features the Commissioner has taken into account in determining the amount of the monetary penalty

---

Nature of the contravention

60. The excel workbooks containing the data were removed by MySociety and cached copies were also removed from the internet.

Effect of the contravention

61. No complaints have been received by the ICO from any of the affected data subjects but complaints were received by the data controller.

Impact on the data controller

62. The liability to pay the monetary penalty will fall on the public purse although the penalty will be paid into the Consolidated Fund.

63. The effect of the contravention is reputational damage and loss of trust by local residents in the data controller's ability to securely manage their data. Further action by the Commissioner will revive the issue, causing further reputational damage to the data controller.

Other considerations

---

64. The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act. This is an opportunity to reinforce the need for data controllers to review their

policies when responding to FOIA requests and to ensure that more secure policies are implemented, and at a minimum, appropriate and effective security measures are applied when responding to FOIA requests.

Notice of Intent

65. A notice of intent was served on the data controller dated 9 July 2013. The Commissioner received written representations from the data controller's Chief Executive dated 30 July 2013. The Commissioner has considered the written representations made in relation to the notice of intent when deciding whether to serve a monetary penalty notice. In particular, the Commissioner has taken the following steps:

- Notes that the data controller has received a number of complaints as a result of the breach which have been managed internally and notes that the data controller, in one case, has received notice of legal action which is currently under review.

- reconsidered the amount of the monetary penalty generally, and whether it is a reasonable and proportionate means of achieving the objective which the Commissioner seeks to achieve by this imposition;

- ensured that the monetary penalty is within the prescribed limit of £500,000; and

- ensured that the Commissioner is not, by imposing a monetary penalty, acting inconsistently with any of his statutory or public law duties and that a monetary penalty notice will not impose undue financial hardship on an otherwise responsible data controller.

Amount of the monetary penalty the Commissioner proposes to impose

---

66. The Commissioner considers that the contravention of section 4(4) of the Act is serious and that the imposition of a monetary penalty is appropriate. Further, he considers that a monetary penalty in the sum of £70,000 is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

67. In reaching this decision, the Commissioner considered other cases of a similar nature in which a monetary penalty has been imposed and the facts and aggravating and mitigating features referred to above. Of particular relevance in this case is the nature of the personal data disclosed, the potential for harm and likelihood of distress.

Payment

68. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 18 September 2013 at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

Early payment discount

69. If the Commissioner receives full payment of the monetary penalty by 18 September 2013 the Commissioner will reduce the monetary penalty by 20% to £56,000 (fifty six thousand pounds).

Right of Appeal

70. There is a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against:

a. the imposition of the monetary penalty and/or;

b. the amount of the penalty specified in the monetary penalty notice.

71. Any Notice of Appeal should be served on the Tribunal by 5pm on 18 September 2013 at the latest. If the notice of appeal is served late the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule. Information about appeals is set out in the attached Annex 1.

72. The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified in the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;

- all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and

- the period for the data controller to appeal against the monetary penalty and any variation of it has expired.

73. In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court.

Dated the 20 August 2013

Signed: ……..

David Smith

Deputy Information Commissioner

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation notice has been served a right of appeal to the (First-tier Tribunal) General Regulatory Chamber (the "Tribunal") against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

GRC & GRP Tribunals
PO Box 9300
Arnhem House
31 Waterloo Way
Leicester
LE1 8DJ

4. The notice of appeal should be served on the Tribunal by 5pm on 18 September 2013 at the latest.

5. If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

6. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

d) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

e) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

7. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

8. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 48 and 49 of,

and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).