PENALTY NOTICE

BIRTHLINK

24 June 2025

DATA PROTECTION ACT 2018

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

PENALTY NOTICE

TO: Birthlink

OF: 21 Castle Street
Edinburgh
EH2 3DN

I. INTRODUCTION AND SUMMARY

1. Pursuant to section 155(1) of the Data Protection Act 2018 ("**DPA**"), the Information Commissioner (the "**Commissioner**") by this written notice ("**Penalty Notice**"), requires Birthlink to pay a monetary penalty of £18,000.

2. This Penalty Notice is given in respect of infringements of the UK General Data Protection Regulation ("**UK GDPR**")[1]. This Penalty Notice contains the reasons why the Commissioner has decided to impose a penalty, including the circumstances of the infringements and the nature of the personal data involved.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
For the period 25 May 2018 to 31 December 2020, references in this Notice to the UK GDPR should be read as references to the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) as it applied in the UK during that period.

3. In accordance with paragraph 2 of Schedule 16 to the DPA, the Commissioner gave a notice of intent to Birthlink on 20 January 2025, setting out the reasons why the Commissioner proposed to give Birthlink a penalty notice. In that notice of intent, the Commissioner indicated that the amount of the penalty he proposed to impose was £45,000.

4. On 12 February 2025, Birthlink sought a short extension of time to make representations. On 25 February 2025, Birthlink made written representations about the Commissioner's intention to give a penalty notice[2]. On 19 March 2025 Birthlink made oral representations about the Commissioner's intention to give a penalty notice at an oral representations meeting.

5. Following the oral representations meeting, on 19 March 2025 Birthlink provided the Commissioner with supplemental information to support the representations made.[3]

6. This Penalty Notice takes into account the entirety of the written and oral representations from Birthlink and where appropriate, makes specific reference to them.

7. Having carefully considered the facts of the case and the Birthlink's representations, the Commissioner finds Birthlink infringed the following provisions of the UK GDPR:

   a. **Article 5(1)(f)** ('integrity and confidentiality' principle)
   b. **Article 5(2)** ('accountability' principle)

[2] Birthlink provided a further risk assessment ("the February 2025 Risk Assessment) as part of the written representations
[3] Missing File Report dated 12 March 2025 and a report on the Birthlink Data Breach entitled "Experiences and impacts of historic forced adoption- a trauma lens".

c. **Article 32(1)-(2)** ('security of processing')

d. **Article 33** ('notification of a personal data breach to the Commissioner')

8. The infringements are set out in detail in this Penalty Notice but in summary:

a. In April 2021, Birthlink destroyed manual records containing personal data of approximately 4,800 of its service users without authorisation or lawful basis ("**Relevant Processing**"). The Relevant Processing affected records that contained sensitive information relating to adoption cases with a Scottish connection, some of which were irreplaceable.[4]

b. The Relevant Processing occurred as a result of Birthlink's failure to implement appropriate organisational measures ensuring the security of the personal data contained in the records. The implementation of such measures would, in all likelihood, have prevented the destruction of the records. In this regard, the Commissioner finds that Birthlink contravened Articles 5(1)(f) and 32(1)-(2) of the UK GDPR.

c. A significant contributing factor leading to the Relevant Processing was Birthlink's failure to demonstrate compliance with the data protection principles in accordance with Article 5(2) of the UK GDPR. Birthlink has accepted that there was limited understanding of the UK GDPR at the time of the

[4] In written representations Birthlink estimated that 10% of files contained irreplaceable items.

Relevant Processing until around March 2023 when it introduced data protection training for its staff.[5]

d. Despite acknowledging the high risk to affected service users arising from the Relevant Processing, Birthlink did not notify the Commissioner of the personal data breach until 8 September 2023. A delay of two years and five months represents a marked departure from the obligation to notify the Commissioner within 72 hours of becoming aware of a personal data breach in accordance with Article 33(1) UK GDPR.

9. In deciding to give this Penalty Notice, the Commissioner has had regard to the matters listed in Articles 83(1)-(2) UK GDPR. The Commissioner is satisfied that the imposition of a financial penalty is an effective, proportionate and dissuasive measure.

10. Having had regard to the matters listed in articles 83(1)-(2) UK GDPR and in accordance with his Data Protection Fining Guidance[6], the Commissioner has determined the amount of the penalty as **£18,000**.

II. LEGAL FRAMEWORK FOR THIS PENALTY NOTICE

11. The legal framework relevant to the Commissioner's findings of infringement of the UK GDPR is produced at Annex 2 to this Penalty Notice.

12. The legal framework relevant to the Commissioner's setting of penalties is set out in Section VI of this Penalty Notice ('**Calculation of penalty**').

III. BACKGROUND TO THE INFRINGEMENTS

[5] Birthlink internal investigation report dated September 2023 at p.11
[6] Data Protection Fining Guidance | ICO, 18 March 2024

13. This section summarises the relevant background to the Commissioner's findings of infringement. It does not seek to provide an exhaustive account of the events that have led to the issue of this Penalty Notice. As set out where relevant below, the Commissioner has taken into account the further information provided by Birthlink in its representations.

A. Birthlink

14. Birthlink is a charity registered with the Office of the Scottish Charity Regulator with charity number SC013007.

15. Since 1984, Birthlink has maintained the Adoption Contact Register for Scotland. This enables adopted people, birth parents, adoptive relatives and birth relatives to register their details with a view to being 'linked' and potentially being reunited.

16. Birthlink primarily provides specialised post-adoption support and advice for adults who have been affected by adoption with a Scottish connection. It also provides similar support and advice to other partner organisations to help people understand their time in care or trace estranged family members (for example, Care Connect Service working with Future Pathways).[7]

17. Birthlink maintains manual records with a view to a 'link' being made on the Adoption Contact Register. The manual records contain the Adoption Contact Register application form (for which there also will be an entry on the digital system). The manual records are stored in filing cabinets

[7] Care Connect Service helps adults who have been in care connect with their past, working with Future Pathways to assist individuals who have been in care locate and understand care records; research and compile family trees; and act as an intermediary to reconnect with family members (see: https://future-pathways.co.uk/meet-the-partner-birthlink/) [last accessed 11 June 2025].

and contain documents relating to an adopted person's individual circumstances. The manual records form part of a 'filing system' pursuant to Article 4(6) UK GDPR.

18. Where a link has previously been made on the Adoption Contact Register for clients of the post-adoption service (i.e. the person searching for their family member has been informed that a match has been made) the manual records are classified by Birthlink as "**Linked Records**".

19. Whilst the personal data contained within the Linked Records in each individual case varies, Birthlink informed the Commissioner that such records may have included:

a. Original birth certificates
b. Adoption Contact Register application form
c. Correspondence between Birthlink and service users
d. Other information relevant to the adoption
e. Irreplaceable items (e.g. handwritten letters from birth parents and birth families, photographs and other sensitive personal information).[8]

B. Destruction of Linked Records

20. Between January and April 2021, [redacted] considered whether there were any barriers to the destruction of the Linked Records to create space within Birthlink's filing cabinets.[9]

[8] Birthlink personal data breach report dated 8 September 2023 at p.3; Birthlink internal investigation report dated September 2023 at pp.1; 15
[9] Birthlink internal investigation report dated September 2023 at pp.1-3; 9

21. A summary of minutes taken at a board meeting on 26 January 2021 indicates that the destruction of Linked Records was raised at board level with the suggestion that the following retention periods should apply to certain files within the Linked Records:[10]

a. **100 years** | Family care and fostering files
b. **Two years** | Adoption support files
c. **One year** | Future Pathways

22. A summary of minutes taken at a management team meeting on 2 February 2021 records that:[11]

a. [redacted] considered there to be no barriers to the destruction of the Linked Records provided that Birthlink maintained adoption and care files for 75 to 100 years;

b. [redacted] consulted with [redacted] on the legality of deleting the Linked Records (although no substantive detail relating to that consultation was recorded); and

c. it was agreed Future Pathways files should also be kept for one year with the remaining Linked Records destroyed.

23. During the Commissioner's investigation, Birthlink was unable to produce any contemporaneous evidence indicating that the board was made aware of the content of the Linked Records. Birthlink accepts that the size and impact of the proposed destruction of Linked Records would

[10] Birthlink internal investigation report dated September 2023 at p.8
[11] Birthlink internal investigation report dated September 2023 at p.2

have required *"clear board approval"* and that this approval does not appear to have been sought.[12]

24. A summary of minutes taken at a management team meeting on 2 March 2021 notes that the destruction of the Linked Records would wait until team members had returned to the office following the Covid period.[13]

25. On 13 April 2021, at a follow-up management meeting it was recorded that the Linked Records would be destroyed on Thursday of that week (i.e. 15 April 2021).[14] No contemporaneous record was kept of the destruction of the Linked Records so Birthlink has determined the date of destruction by reference to these meeting minutes only.[15]

26. A summary of minutes taken at a management team meeting on 25 May 2021 notes that the Linked Records had been 'culled' but not destroyed on 15 April 2021. The minutes note that 40 bags of Linked Records were ready to be shredded on Thursday of that week (i.e. 27 May 2021).

27. By its own admission, Birthlink accepts that there was limited understanding of the UK GDPR within the organisation. At the time, it had not implemented any data protection policies or procedures[16] and its staff had not received any data protection training. Such training was not provided to staff until March 2023.[17]

28. In the absence of appropriate policy documents and relevant board approval, the decision to destroy the Linked Records was left to

[12] Birthlink internal investigation report dated September 2023 at pp.11-12
[13] Birthlink internal investigation report dated September 2023 at p.2
[14] Birthlink internal investigation report dated September 2023 at p.2
[15] Birthlink internal investigation report dated September 2023 at p.2
[16] Birthlink response to ICO dated 24 November 2023 at [23-25]
[17] Birthlink internal investigation report dated September 2023 at p.11

[redacted] who had not received any formal data protection training.

29. In the circumstances, the destruction of the Linked Records had not received the relevant approval and was therefore unauthorised.

C. Birthlink's Internal Investigation and Notification

30. The Relevant Processing was brought to the attention of Birthlink's Interim Chief Executive Officer following a *"short notice inspection"* by the Care Inspectorate which took place between 23 and 29 August 2023, and completed on 5 September 2023. In its report, the Care Inspectorate noted:

    a. There had been a *"significant loss of information provided by people who use the service… which has the capacity to impact people's experiences and outcomes seriously and negatively"*.[18]

    b. The information lost was *"crucial information"*.[19]

    c. Birthlink *"did not take a comprehensive approach in relation to risk management and planning in respect of this activity, giving due consideration to the special nature of the information held"*.[20]

31. As a result of its findings, the Care Inspectorate required Birthlink to carry out a review of the Relevant Processing by 15 December 2023.

32. Following the conclusion of the Care Inspectorate's inspection, Birthlink:

[18] Care Inspectorate Report dated 5 September 2023 at p.3 (available at: https://www.careinspectorate.com/berengCareservices/html/reports/getPdfBlob.php?id=316903) ("**Care Inspectorate Report**") [last accessed 11 June 2025]
[19] Care Inspectorate Report at p.6
[20] Care Inspectorate Report at p.6

a. notified the Commissioner of a personal data breach on 8 September 2023; and

b. conducted an internal investigation into the Relevant Processing[21] (the findings of which were reported to the Commissioner in October 2023).

33. As part of its internal investigation, Birthlink reviewed contemporaneous documentary material relating to the Relevant Processing and obtained personal accounts from the members of staff involved. The findings of the internal investigation highlight the following relevant points:

a. The [redacted] consulted by [redacted] prior to the Relevant Processing recalled being "*very clear that* [redacted] *should only destroy records that could be replaced (i.e. records found in national databases) and that they should set a realistic retention period".*[22]

b. The [redacted] also recalled informing [redacted] that "*it would take time to go through files"* and "*suggested a list of all types of paperwork that could be contained in the files be created, then use that list to note what could and couldn't be destroyed".*[23]

c. At the time of the Relevant Processing, [redacted] felt "*uncomfortable shredding people's photographs and cards"* and raised their concerns with [redacted]. In response to

[21] Birthlink internal investigation report dated September 2023
[22] Birthlink internal investigation report dated September 2023 at p.8
[23] Birthlink internal investigation report dated September 2023 at p.8

those concerns, [redacted] was told *"it needed to be done"*.[24]

d. Contrary to the views of [redacted] who was consulted, [redacted] recalled there being *"no thorough check of what was on the files"* – they were *"just ripped out and put in bags"*.[25]

e. The [redacted] noted that they were *"unaware that non-replaceable personal items such as letters from birth parents had been destroyed"* or that *"entire files were destroyed without being reviewed"* contrary to their previous advice.

34. The Commissioner acknowledges that the personal accounts provided during Birthlink's internal investigation post-date the Relevant Processing by two years and five months. The Commissioner has taken this into consideration when assessing the weight to place on such accounts.

D. Impact of the Relevant Processing

Affected individuals

35. In its notification to the Commissioner, Birthlink admits that it does not know how many individuals may have been affected.[26] In response to the Commissioner's enquiries, Birthlink estimated that the Linked Records may have included personal data of approximately 4,800 individuals.[27]

[24] Birthlink internal investigation report dated September 2023 at p.9
[25] Birthlink internal investigation report dated September 2023 at p.9
[26] Birthlink personal data breach report dated 8 September 2023 at p.3
[27] Birthlink response to ICO dated 24 November 2023

36. In the absence of any record relating to the Relevant Processing, Birthlink estimated the number of files destroyed based on the following assumptions:

    a. 24 drawers of filing cabinets containing Linked Records were destroyed; and

    b. each drawer contained approximately 200 records.[28]

37. The estimated number provided by Birthlink only represents the identifiable individuals to which the Linked Records relate. In practice, each Linked Record will have contained personal data relating to other 'linked' individuals, the number of which was described to the Commissioner as "*incalculable*".[29]

38. In its written representations, Birthlink told the Commissioner that:

    "*Due to historic record keeping practices, regrettably it is not possible to absolutely know how many people have been impacted or indeed who those people are. Birthlink are deeply sorry that this is the situation*". [30]

    Impact on affected individuals

39. In its notification to the Commissioner, Birthlink highlighted the serious nature of the Relevant Processing for its service users, as follows:

    "Amongst the documents shredded were irreplaceable handwritten letters from parents to their children who were adopted away from

[28] Birthlink responses to ICO dated 24 November 2023 at [4]
[29] Birthlink response to ICO dated 24 November 2023 at [4]
[30] Birthlink written representations dated 25 February 2025

them. Photographs of babies were destroyed. The significance of these documents cannot be underestimated. People will no longer have access to them. [redacted]".[31]

40. The Care Inspectorate Report assessed the risk to Birthlink's service users as *"high"* noting that their *"sense of identity and history will be severely compromised by [the] loss of historical information".*[32]

41. The Care Inspectorate's assessment is echoed by the findings of Birthlink's internal investigation, which summarised the risks to affected individuals in the following way:

"There is a high, and inevitable risk that service users' sense of identity and understanding of their family history will be compromised. [redacted]".[33]

42. In its written representations, Birthlink confirmed that its initial understanding of the likely number of Linked Records containing cherished or irreplaceable items (that is Linked Records containing the only available source of that personal data) was not accurate:

[31] Birthlink personal data breach report dated 8 September 2023notification at pp.3-4
[32] Care Inspectorate Report at p.3
[33] Birthlink internal investigation report dated September 2023 at p.14

"*On reflection, our initial representation of the breach to the Commissioner was based on organisational memory of the event and our understanding of what a cherished item was. Recent consideration to content of records through file sampling has brought to light that the criteria of cherished (irreplaceable) items is not aligned with the archive communities understanding of what constitutes a cherished item. The onboarding of* [redacted] *to the organisation has allowed us to reappraise with their subject matter expertise what truly constitutes a cherished item or memory. Items considered as cherished include:*

- *Handwritten letters from birth Mothers and Fathers to their children*
- *Handwritten letters from birth families to their sibling*
- *Photographs*
- *Information disclosed during the research period that are not documented elsewhere"*[34]

43. Birthlink submitted in its written and oral representations that file sampling has identified evidence of these cherished items being given to individuals when a link was made. Birthlink now estimates that the total number of Linked Records containing cherished items that could not be replaced may "*be less than 10%*".[35]

44. On 19 March 2025, Birthlink provided a report to the Commissioner entitled "Experiences and impacts of historic forced adoption- a trauma lens". This opening paragraph of this report summarises Birthlink's current understanding of the impact on affected individuals as follows:

[34] Birthlink written representations dated 25 February 2025
[35] Birthlink written representations dated 25 February 2025

"On 15 April 2021 a large quantity of files was destroyed. For a small (unknown) number of people this included irreplaceable items. This was not a trauma informed decision. The agency has not kept these items reliably and has significantly disempowered the people served. Included in the destruction were photographs and letters from parents to their adopted children."

Communicating with affected individuals

45. In its Personal Data Breach Report, Birthlink told the Commissioner that it had contacted the individuals affected.[36]

46. In response to the Commissioner's enquiries, Birthlink clarified its position noting that only individuals returning to Birthlink for another service and identified as being affected by the breach had been notified. Birthlink confirmed that without a record of the Linked Records that had been destroyed, it was not able to communicate the breach to the remaining affected individuals.[37] Birthlink is reliant on individuals searching for information on a Linked Record before it is able to determine whether the individual has been affected by the Relevant Processing. Where that is the case, Birthlink has informed the Commissioner that it is employing a duty of candour protocol to explain to service users that the Linked Record cannot be located.

47. The Commissioner acknowledges that Birthlink did consider whether it would be appropriate to make a public communication regarding the Relevant Processing.

[36] Birthlink personal data breach report dated 8 September 2023 at p.4
[37] Birthlink response to ICO dated 24 November 2023 at [1]

48. Birthlink was asked to provide further representations on the appropriate ways it could have communicated the personal data breach to affected data subjects. In its representations, Birthlink identified three potential approaches and provided representations on the impact and outcome of these approaches, namely:

a. Communicating with all people recorded in the Adoption Contact Register (Approximately 32,000 people);
b. Communicating to the general public using prominent website banners or notifications or prominent advertisements in print media;
C. Communicating on an individual tailored approach to people who have historically been supported by Birthlink and return for further services.[38]

49. In its written representations Birthlink outlined the ethical and practical difficulties of communicating with all people recorded in the Adoption Contact Register.

50. Birthlink told the Commissioner that it had not communicated the data breach to the general public as, amongst other reasons, it did not want "*people to think they had cherished and irreplaceable items on file when this was not the case,* [redacted]".[39]

51. Birthlink had therefore elected for an individual tailored approach, communicating the data breach to people who have historically been supported by Birthlink and they return for further services.[40] Birthlink

[38] Birthlink written representations dated 25 February 2025
[39] Birthlink written representations dated 25 February 2025
[40] Birthlink written representations dated 25 February 2025

believes that this has allowed a "*trauma sensitive and person-centred approach*".[41]

IV. THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

A. Controllership and jurisdiction

52. Recital 15 UK GDPR provides that the *"protection of natural persons should apply to… manual processing, if the personal data are contained or are intended to be contained in a filing system"*.

53. The Linked Records were stored in filing cabinets and were, for the proper operation of the services offered by Birthlink, able to be retrieved according to specific criteria. The Linked Records therefore formed part of a 'filing system' as defined by Article 4(6) UK GDPR.

54. Based on the nature of the Linked Records, the purposes for which they were held, and the categories of documents they were likely to contain, the Commissioner is satisfied that the Linked Records contained personal data within the meaning of Article 4(1) UK GDPR.

55. Birthlink is the controller in respect of its processing of personal data contained within the Linked Records. It determines the purposes and means by which that personal data is processed within the meaning of Article 4(7) UK GDPR.

56. The Relevant Processing (i.e. the destruction) of the Linked Records was an act of processing the personal data contained within those records within the meaning of Article 4(2) UK GDPR.

[41] Birthlink written representations dated 25 February 2025

57. The UK GDPR applied to the Relevant Processing by virtue of Article 2(1) (as supplemented by Article 2(5)(a)(ii)) UK GDPR and Article 3(1) UK GDPR. That is:

    a. the Relevant Processing was structured processing of personal data forming, or intended to form, part of a filing system;

    b. it took place in the context of the activities of a controller established in the UK; and

    c. none of the exceptions in Article 2 UK GDPR apply.

58. Part 2 of the DPA applied to the Relevant Processing by virtue of section 4 DPA.

B. Nature of the personal data and context of the processing

59. The Linked Records formed part of Birthlink's maintenance of the Adoption Contact Register for Scotland and its provision of specialist post-adoption support.

60. Birthlink addressed the nature of the Linked Records in its written representations. The February 2025 Risk Assessment, records that:

"The destroyed records were classed as 'linked' files. What this means in practice is that a link with a family member has been made on the adoption contact register (ACR). The person searching for their family member will have been informed that a match has been made on the ACR and supported to make decisions about what to do next. The person then has it within their power to decide whether to connect with

their family member or not. The person will have received copies of their information."

61. At the oral representations meeting, Birthlink's [redacted] provided further representations on the role of the "linked records" which were destroyed. The minutes of the meeting record that:

"the destroyed files were all likely to be 'linked' files because of the way they were stored. In this case a match will have been made through the Adoption Contact Register (ACR) and the individuals will have been communicating with each other. Those files were then closed and would only have been reopened again if the person came back to Birthlink wanting to find another family member." [42]

62. The Commissioner accepts the representations from Birthlink that the Linked Records are likely to have been records where a link had been made through the Adoption Contact Register.

63. Whilst some of the documents contained in the Linked Records will have been given to the individual when a link was made and some will be replaceable from public records (e.g. birth certificates), other documents containing personal data (including the personal data contained in cherished or irreplaceable items) are likely to have been destroyed.

64. The internal investigation report from Birthlink dated September 2023[43] records that [redacted] involved in the destruction of the Linked Records in April 2021 reported feeling "*uncomfortable shredding people's photographs and cards*".[44]

[42] Minutes of oral representations meeting 19 March 2025
[43] Provided to the ICO as Appendix 9- Investigation Birthlink File Destruction April 2021
[44] Birthlink internal investigation report dated September 2023

65. Birthlink told the Commissioner that, in some cases, the Linked Records *"will have contained the only reference anywhere in the world to the paternity of adopted children"*.[45]

66. Whilst Birthlink now estimates that the total number of Linked Records containing irreplaceable items may *"be less than 10%"*[46] the weight which can be placed on this figure is limited. Birthlink does not know the exact nature of the Linked Records destroyed so cannot say with certainty that the files sampled by [redacted] are comparable to those which were destroyed.

67. The Commissioner is satisfied that some of the Linked Records will have contained irreplaceable items (e.g. handwritten letters from birth parents and birth families, photographs and other sensitive personal information).

68. However, as Birthlink did not document the Linked Records which were destroyed it is therefore not possible to definitively determine which Linked Records (including the documents and personal data contained within them) were lost due to the Relevant Processing.

C. The infringements | Articles 5(1)(f) and 32(1)-(2) UK GDPR

69. The Commissioner has considered whether the facts set out in paragraphs 20 to 34 above constitute infringements of Articles 5(1)(f) and 32(1)-(2) UK GDPR. The relevant text of those provisions is reproduced in Annex 2 to this Penalty Notice.

[45] Birthlink personal data breach report dated 8 September 2023 at p.3
[46] Birthlink written representations dated 25 February 2025

70. In order to assess Birthlink's compliance with Articles 5(1)(f) and 32(1)-(2) UK GDPR, the Commissioner must necessarily exercise his judgement, as the regulator, as to what "*appropriate*" security and "*appropriate*" organisational measures would be in the circumstances (that is, taking into account "*the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*").

71. For the reasons set out below, the Commissioner's view is that Birthlink infringed Articles 5(1)(f) and 32(1)-(2) UK GDPR. The infringements involved Birthlink's failure to use appropriate organisational measures to ensure the appropriate security of the personal data from the Relevant Processing.

Appropriate security of the personal data

72. In assessing the "*appropriate security of the personal data*" under Article 5(1)(f) UK GDPR (and, equivalently, the "*level of security appropriate to the risk*" under Article 32 UK GDPR), the Commissioner has considered the risk to the rights and freedoms of Birthlink's service users which the Relevant Processing presented. Recital 75 UK GDPR states that such risk "*may result from personal data processing which could lead to physical, material or non-material damage*".

73. As explained at paragraphs 39 and 41 above, Birthlink informed the Commissioner that the destruction of the Linked Records presents a high and inevitable risk to affected service users. Those risks include:

[redacted]

74. The Commissioner considers all three categories of damage as identified in Recital 75 UK GDPR (physical, material and non-material) would be likely to flow from the risks identified at paragraph 73 above.

75. The Commissioner acknowledges that neither he nor Birthlink have received any complaints in relation to the Relevant Processing. However, little weight can be placed on the absence of complaints in circumstances where Birthlink has not been able to communicate the personal data breach to affected individuals and has not communicated the personal data breach more widely. Publicly communicating the personal data

[47] Care Inspectorate Report at p.3
[48] Birthlink personal data breach report dated 8 September 2023 at pp.3-4
[49] Birthlink internal investigation report dated September 2023 at p.14
[50] Birthlink internal investigation report dated September 2023 at p.14

breach would have enabled service users to come forward and enquire whether their personal data had been affected.[51]

76. Based on the risks identified at paragraphs 39 to 41 and 73 above, the Commissioner considers the severity of the risks associated with the Relevant Processing to be high.

77. In respect of the likelihood of risk, Birthlink should have been aware that any unauthorised access to, loss or destruction of, the Linked Records, was likely to pose a significant risk to rights and freedoms of its service users.

78. The factors identified above indicate that a high level of security was appropriate to the risk presented by the general processing of Linked Records (e.g. storage and retention) and, in particular, the Relevant Processing. Birthlink was therefore required to implement appropriate organisational measures to ensure a high level of security.

Assessment of compliance

79. Under the UK GDPR, it is for Birthlink to demonstrate compliance with Article 5(1)(f) (by virtue of Article 5(2)). It is also for Birthlink to demonstrate compliance with Article 32(1) and (2) UK GDPR (by virtue of Article 24).

80. The Commissioner finds that the Linked Records destroyed by the Relevant Processing were not processed in a manner that ensured the

[51] Birthlink written representations 25 February 2025 record that Birthlink recognises that publicly communicating the breach could "*offer opportunities for duty of candour to be undertaken*" although this would need to be balanced against the risks that people may think they had cherished and irreplaceable items on file destroyed when this was not the case, discussed below at paragraphs 154-158. 154

appropriate security of the personal data (including protection against unauthorised destruction).

81. The Commissioner's Security Guidance[52] explains:

> *"Every aspect of your processing of personal data is covered, not just cybersecurity. This means the security measures you put in place should seek to ensure that:*
>
> - *the data can be accessed, altered, disclosed or deleted only by those you have authorised to do so (and that those people only act within the scope of the authority you give them);*
>
> *…*
>
> - *the data remains accessible and usable, ie, if personal data is accidentally lost, altered or destroyed, you should be able to recover it and therefore prevent any damage or distress to the individuals concerned"*.

82. Since, at least, 25 May 2018 (the date on which the DPA and the UK GDPR[53] came into force), Birthlink should have implemented appropriate policies, procedures and training to demonstrate compliance with UK GDPR. This was particularly important with regards to its processing of Linked Records and the efficacy of the services it offers to its users. For the reasons provided at paragraphs 73 to 77 above, Birthlink ought to have been aware of the high risk of damage and distress likely to be

[52] Dated 19 May 2023 (available at: https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security-0-0.pdf) [last accessed 23 October 2024]

[53] For the reasons set out at footnote 1 above, for the period 25 May 2018 to 31 December 2020, references in this Notice to the UK GDPR should be read as references to the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) as it applied in the UK during that period.

caused to its service users if Linked Records were destroyed without authorisation or were otherwise lost.

83. From, at least, 25 May 2018 until remedial action was taken by Birthlink (starting in March 2023 and then following the Care Inspectorate Report dated 5 September 2023), Birthlink failed to implement:

a. A data retention policy [54]
b. A data destruction policy
c. Any sufficient internal approval process for the destruction of Linked Records
d. Any data protection training for members of staff[55]

84. These organisational measures could have been implemented at minimal cost and would have, in all likelihood, prevented the unauthorised destruction of Linked Records.

85. Furthermore, Birthlink has not provided the Commissioner with any evidence demonstrating it had assessed the risk posed to personal data contained in the Linked Records or how valuable, sensitive or confidential the personal data was for the purposes for which it was processed (as required by Article 32(2) UK GDPR).

86. In the absence of any assessment of the risks posed to personal data contained in Linked Records and the implementation of any organisational measures to ensure the security of such personal data,

[54] A data retention policy was first put in place in March 2023 (Birthlink written representations 25 February 2025)
[55] Data protection training for staff was introduced in March 2023 (Birthlink written representations 25 February 2025)

the Commissioner finds Birthlink has infringed Articles 5(1)(f), 32(1) and 32(2) of the UK GDPR.

D. The infringements | Article 5(2) UK GDPR

87. The Commissioner has also considered whether Birthlink has infringed Article 5(2) UK GDPR. The text of Article 5(2) is reproduced in Annex 2 to this Penalty Notice.

88. Article 5(2) UK GDPR imposes a dual requirement on controllers:

a. Firstly, to be responsible for compliance with the data protection principles.

b. Secondly, to demonstrate compliance with those principles.

89. During the Commissioner's investigation, Birthlink explained that it had not implemented organisational measures (such as those set out in paragraph 83 above) and that it had a limited understanding of the UK GDPR. At the relevant time, Birthlink also:

a. failed to maintain a record of its processing activities (Article 30 UK GDPR);

b. did not undertake any data protection impact assessments for any of its high-risk processing activities (Article 35 UK GDPR); and

c. did not have an appointed data protection officer (Article 37 UK GDPR).

90. In the absence of basic organisational measures safeguarding personal data contained within the Linked Records and any record of processing activities, Birthlink has been unable to demonstrate its responsibility for compliance with the data protection principles. In particular:

    a. Article 5(1)(a) ('lawfulness fairness and transparency' principle)
    b. Article 5(1)(e) ('storage limitation' principle)
    c. Article 5(1)(f) ('integrity and confidentiality' principle)

91. The appointment of a data protection officer would have provided Birthlink with a specialist resource. A data protection officer would have recognised the importance of implementing appropriate policies and procedures, conducting data protection impact assessments, and implementing appropriate organisational measures. By not appointing such a resource Birthlink's decision to undertake the Relevant Processing was left to managers without any formal data protection training and/or guidance and led to the destruction of private and sensitive personal data.

92. Whilst Birthlink has now appointed a data protection officer and has made meaningful progress in implementing important measures to bring its data protection into compliance, in April 2021 it is accepted that the Relevant Processing was "*not well governed, controlled or documented*".[56]

Demonstrating compliance with Article 5(1)(a) UK GDPR

93. The lawfulness, fairness and transparency principle requires compliance with three further provisions of the UK GDPR:

[56] Birthlink representations, February 2025 Risk Assessment

a. **Article 6** ('lawfulness of processing')
b. **Article 9** ('processing of special category of data')
c. **Article 12** ('transparent information, communication and means of data subjects exercising their rights')

94. Birthlink has not been able to demonstrate a lawful basis for the Relevant Processing under Articles 6 and 9 UK GDPR (as appropriate). This is compounded by Birthlink's failure to maintain a record of its processing activities in accordance with Article 30 UK GDPR. A record of processing activities would have assisted Birthlink to take responsibility for retention and destruction of Linked Records and demonstrate a lawful basis for the Relevant Processing.

95. Furthermore, Birthlink provided the Commissioner with a copy of its privacy notice dated November 2020 during his investigation. It referred to the storage of personal data but did not provide any information on the length of time the personal data would be retained or that it would be destroyed after a specified period.

96. By not having a privacy notice informing people how long their personal data would be retained for and how it would be destroyed when it was no longer necessary, Birthlink did not demonstrate compliance with the transparency requirements of Article 5(1)(a).

Demonstrating compliance with Article 5(1)(e) UK GDPR

97. Demonstrating compliance with Article 5(1)(e) UK GDPR required Birthlink to implement appropriate policies and procedures relating to the retention of Linked Records and the destruction of such records.

98. Without a data retention policy, Birthlink was not able to demonstrate personal data was no longer necessary for the purpose for which it was obtained (and could therefore be destroyed in accordance with a data destruction policy).

99. A data retention policy would have assisted Birthlink in identifying the personal data which had been destroyed. This would, in turn, have supported appropriate communication with data subjects and with the Commissioner. This failure has had significant consequences for both Birthlink and data subjects and underscores the critical importance of data protection compliance and accountability.

Demonstrating compliance with Article 5(1)(f) UK GDPR

100. Similarly, in the absence of appropriate policies, procedures and staff training, Birthlink was not able to demonstrate compliance with its obligations under Article 5(1)(f) UK GDPR or how it was taking responsibility for such compliance. Birthlink's failure to comply with Article 5(1)(f) UK GDPR is considered at paragraphs 69 to 86 above.

E. The infringements | Article 33 UK GDPR

101. The text of Article 33(1) UK GDPR is reproduced in Annex 2 to this Penalty Notice.

102. By Article 33(1) UK GDPR controllers must notify the Commissioner within 72 hours of becoming aware of a personal data breach unless it is unlikely to result in a risk to the rights and freedoms of natural persons. The Commissioner considers that the Relevant Processing constituted a

notifiable personal data breach and Birthlink was under an obligation to notify the Commissioner.

103. In its representations, Birthlink told the Commissioner that "p*eople did not identify it as a data breach at the time and did not see it necessary to report*".[57]

104. This is not an adequate justification for the failure to notify the Commissioner. The UK GDPR puts an obligation on data controllers to have appropriate technical and organisational measures in place to quickly detect if a data breach has occurred. Birthlink cannot rely on its failure to implement appropriate technical and organisational measures as a justification for not identifying and reporting a personal data breach.[58]

105. A personal data breach is defined by Article 4(12) UK GDPR and includes *"a breach of security leading to the accidental or unlawful destruction [or] loss… of personal data"*.

106. Service users provided their personal data to Birthlink in the expectation that their data would be held securely. This is particularly so in circumstances where Birthlink was entrusted with documents which contained highly sensitive and sentimental personal data. On that basis, it ought to have been clear to Birthlink that the destruction of the Linked Records constituted a personal data breach that was required to be notified to the Commissioner.

[57] Birthlink written representations 25 February 2025
[58] The WP29 Guidelines on Personal Data Breach Notification (Guidelines 9/2022) explains that the GDPR "*…requires the controller to implement all appropriate technical protection and organizational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects….. This puts an obligation on the controller to ensure that they will be 'aware' of any breaches in a timely manner so that they can take appropriate action*." [58] WP29 has been replaced by the European Data Protection Board (EDPB). Although these guidelines relate to the EU version of the GDPR, they are a useful resource for understanding the requirements of the UK GDPR.

107. Birthlink initially told the Commissioner that the risk to affected individuals is high[59]. Birthlink therefore ought to have recognised that the Article 33(1) UK GDPR threshold for making such a notification had been met.

108. As part of its written representations, Birthlink submitted the February 2025 Risk Assessment. In this risk assessment, the likelihood of harm was assessed as "medium". Birthlink explained that the likelihood of harm in the risk matrix submitted was assessed on the basis that "*no individuals have come back to Birthlink in 4 years and subsequently been identified as having cherished items missing*". The Commissioner does not accept that this is a proper assessment of the likelihood of the risks to data subjects and is not a sufficient risk assessment for the purposes of Article 33 UK GDPR. In assessing risk in accordance with the requirements of Article 33 UK GDPR, a controller must have regard objectively both to the likelihood and severity of the risk to the rights and freedoms of data subjects. An assessment with the benefit of hindsight based on the small number of data subjects informed[60] by Birthlink that files had been destroyed is not an objective assessment of the potential adverse consequences for individuals from the destruction of the Linked Records.

109. It was Birthlink's responsibility to assess the Relevant Processing and determine whether it met the threshold for notification to the Commissioner as required by Article 33(1) UK GDPR. It failed to do so.

[59] Birthlink personal data breach report dated 8 September 2023
[60] The Missing File Report submitted by Birthlink to the ICO on 19 March 2025 outlined 5 case studies where a file was missing and deemed to be destroyed.

110. Birthlink did not notify the Commissioner within 72 hours of becoming aware of the personal data breach (i.e. when the personal data contained in the destroyed Linked Records was no longer accessible). The personal data breach was only reported to the Commissioner two years and five months later following the publication of a report by the Care Inspectorate (see paragraphs 30 to 32).

111. The Commissioner therefore finds Birthlink infringed Article 33(1) UK GDPR.

V. DECISION TO IMPOSE A PENALTY

A. Legal Framework | Penalties

112. When deciding whether to issue a penalty notice, and determining the appropriate amount of that penalty, section 155(2)(a) DPA requires the Commissioner to have regard to the matters listed in Articles 83(1) and 83(2) UK GDPR, insofar as they are relevant in the circumstances of the case.

113. Article 83(1) UK GDPR requires any penalty imposed by the Commissioner to be effective, proportionate, and dissuasive in each individual case.

114. Article 83(2) UK GDPR requires the Commissioner to have due regard to the following factors when determining whether to issue a penalty notice and the appropriate amount of any such penalty in each individual case:

> *"(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*

(b) the intentional or negligent character of the infringement;

(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the Commissioner, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement".

B. The Commissioner's Decision on whether to Impose a Penalty

115. Paragraphs 117 to 174 below set out the Commissioner's assessment of whether it is appropriate to issue a penalty in relation to the five infringements set out above. That assessment involves consideration of the factors in Articles 83(1) and 83(2) UK GDPR. The order in which these considerations are set out below follows the Commissioner's Data Protection Fining Guidance ("**Fining Guidance**"):[61]

    a. **Seriousness of the infringements** (Article 83(2)(a), (b) and (g))
    b. **Relevant aggravating or mitigating factors** (Article 83(2)(c)-(f), (h)-(k))
    c. **Effectiveness, proportionality and dissuasiveness** (Article 83(1))

116. The Commissioner has not conducted a separate assessment for each of the infringements. He considers the infringements of Articles 5(1)(f), 5(2), 32(1) and 32(2) relate to the same processing operations. Whilst the failure to report the personal data breach under Article 33 is a separate infringement, in the circumstances of this case, the Commissioner considers that failure to be linked to the lack of appropriate technical and organisational measures and the failure to demonstrate compliance with the data protection principles.[62] An

[61] Dated 15 March 2024 (available at: https://ico.org.uk/about-the-ico/our-information/policies-and-procedures/data-protection-fining-guidance/) [last accessed: 10 June 2025]
[62] For the avoidance of doubt, the Commissioner considers Articles 5(1)(f), 5(2), 32(1), 32(2) and 33 UK GDPR to be evidently distinct provisions of the UK GDPR. Had the Commissioner calculated penalties for infringements of these provisions separately, he would have had to ensure, in accordance with Article 83(3) UK GDPR, that the total penalty did not exceed the amount specified for the gravest infringement (that of Article 5(1)(f) UK GDPR). However, in this Notice the Commissioner has exercised his discretion and decided to calculate a single penalty.

assessment of whether it is appropriate to issue a penalty has therefore been taken in relation to the infringements collectively.

Seriousness of infringements | Article 83(2)(a) the nature, gravity and duration of the infringements

117. In assessing the seriousness of the infringements, the Commissioner has given due regard to their nature, gravity and duration.

Nature of the infringements

118. Article 5(1)(f) and 5(2) UK GDPR are core principles of processing personal data. Infringements of these principles are subject to the higher maximum fine[63] reflecting the seriousness of such infringements.

119. Infringements of Articles 32(1), 32(2) and 33(1) UK GDPR are subject to the standard maximum fine.[64]

120. The nature of the personal data and the context of the Relevant Processing is set out at paragraphs 59 to 68 above. In the Commissioner's view, the absence of appropriate organisational measures to ensure an appropriate level of security presented a high risk to underlying individuals. The risk materialised on 15 April 2021.

121. The Commissioner has identified infringements of four provisions of the UK GDPR which led to the unauthorised destruction of personal data (see

[63] £17,500,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(5) UK GDPR).
[64] £8,700,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(4) UK GDPR).

paragraphs 69 to 111 above). Birthlink accepts that there was limited understanding of the UK GDPR at the time of the Relevant Processing.[65]

122. The infringement of Article 33(1) UK GDPR not only relates to Birthlink's failure to notify the Commissioner of the personal data breach within 72 hours of becoming aware of it, it represents a failure to implement appropriate measures to establish whether a personal data breach had actually occurred.[66] Birthlink accepts that its staff had not undergone any formal data protection training prior to March 2023 at which time such training was introduced.[67] This illustrates the interconnection between Birthlink's infringement of Article 33(1) UK GDPR and its accountability failings under Article 5(2) UK GDPR.

123. Birthlink's limited understanding of core principles of data protection law increases the seriousness of the infringements.

Gravity of the infringements

124. In assessing the gravity of the infringements, the Commissioner has considered the nature, scope and purpose of the Relevant Processing, as well as the number of data subjects affected by the Relevant Processing and the level of damage they have suffered.[68]

125. The Commissioner notes that Article 83 UK GDPR has a punitive purpose and is not conditional on evidence of actual harm to data subjects.[69]

[65] Birthlink internal investigation report dated September 2023 at p.11
[66] Recital 87 UK GDPR
[67] Birthlink internal investigation report dated September 2023 at p.11
[68] Article 83(2)(a) UK GDPR
[69] UI v. Österreichische Post AG (C-300/21) EU:C:2023:370 at [40]. The Commissioner accepts that the operation of section 6 European Union (Withdrawal) Act 2018 means that European case law is no longer binding on domestic courts. However, domestic courts may still have regard to decisions of the Court of Justice of the European Union insofar as such decisions are relevant to matters before them.

126. **Nature and purpose of processing** | The nature and purpose of Birthlink's processing of the personal data contained in Linked Records is explained at paragraphs 59 to 68 of this Penalty Notice. The Commissioner acknowledges that the processing activities should be viewed in the context of Birthlink furthering its charitable purposes but nevertheless finds:

i. Service users provided personal data (some highly sensitive and sentimental) to Birthlink in the expectation that their data would be held securely for the purpose of establishing a link between birth and adoptive relatives. In some cases, birth parents entrusted Birthlink with irreplaceable handwritten letters and photographs intended for their children that had been placed for adoption.[70]

ii. The personal value of the services offered by Birthlink was high. In its report, the Care Inspectorate highlighted the nature and quality of the support which Birthlink provided to its users with one user commenting that *"my life has been transformed significantly by Birthlink"*.[71]

iii. In the absence of appropriate security measures, and in the event of a personal data breach, the nature of Birthlink's processing was likely to result in a high risk to data subjects. Paragraph 73 above contains a summary of the complex impact the Relevant Processing may have on affected individuals.

[70] Birthlink personal data breach report dated 8 September 2023 at pp.3-4
[71] Care Inspectorate Report at p.4

iv. The highly sensitive and sentimental nature of some of the personal data likely to have been destroyed by the Relevant Processing adds to the seriousness.

127. **Scope of processing** | In regard to the scope of Birthlink's processing activities, the Commissioner notes that:

i. The territorial scope of the processing is broad. Birthlink's processing of personal data within Linked Records is for the purpose of maintaining the Adoption Contact Register and providing services to partner organisations. The Adoption Contact Register was established in 1984 and relates to adoption cases with a Scottish connection.

ii. Birthlink did not maintain records of the Relevant Processing but estimates that the Relevant Processing is likely to have affected 4,800 Linked Records. However, Birthlink has told the Commissioner that the number of affected data subjects is *"incalculable"*.

iii. The failure to maintain a record of the Relevant Processing and to determine the identities of the affected data subjects (particularly in circumstances where there is a high likelihood of complex harm arising) increases the seriousness.

Duration of the infringements

128. **Articles 5(1)(f), 5(2) and 32(1)-(2) UK GDPR** | The Commissioner finds that the duration of the infringements was from, at least, 25 May 2018 (the date on which the DPA and the GDPR (now UK GDPR) came into force) until remedial action was taken by Birthlink following the Care Inspectorate Report dated 5 September 2023[72].

129. **Article 33 UK GDPR** | The Commissioner finds that the infringement was from 18 April 2021 (i.e. 72 hours after the Relevant Processing) until 8 September 2023 (i.e. the date on which Birthlink notified the Commissioner of the personal data breach). A delay of two years and five months represents a marked departure from the obligation to notify the Commissioner within 72 hours in accordance with Article 33(1) UK GDPR.

Conclusion on nature, gravity and duration of the infringements

130. The nature, gravity and duration of the infringements all increase the seriousness of the infringements.

Seriousness of infringements | Article 83(2)(b) the intentional or negligent character of the infringements

131. In its notification to the Commissioner, Birthlink highlighted it was an *"intentional decision at the time to destroy records"*.[73] The Commissioner, however, finds the infringements not to have been intentional.

[72] Although data protection training and retention policies were implemented in March 2023, the infringements continued until appropriate technical and organisational measures were implemented following the Care Inspectorate Report dated 05 September 2023.
[73] Birthlink personal data breach report dated 8 September 2023 at p.2

132. In reaching this finding, the Commissioner has viewed the infringements in the context of Birthlink's failure to demonstrate compliance with data protection principles and its admission that it had a limited understanding of data protection law at the relevant time.

133. Whilst the [redacted] may have intended to destroy the Linked Records, the Commissioner considers that, in doing so, they did not intend to contravene data protection law. At paragraphs 20 to 22 above, it is noted that [redacted] did give consideration to barriers that may prevent the destruction of the Linked Records (although no contemporaneous detail of those considerations is available).

134. The Commissioner has considered the personal accounts from the members of staff involved but has placed limited weight on them given the two year and five month delay in obtaining those accounts.

135. In the circumstances, had Birthlink provided data protection training for its staff and implemented appropriate policies and procedures for staff to follow, the managers would have had a greater awareness of what they could and could not do with the Linked Records.

136. The implementation of appropriate policies and procedures would also have enabled Birthlink's staff to recognise that the Relevant Processing was a personal data breach and that it had an obligation to make a notification to the Commissioner.

137. The Commissioner is therefore satisfied that the Relevant Processing was negligent, not intentional.

Seriousness of infringements | Article 83(2)(g) categories of personal data affected

138. In its notification to the Commissioner, Birthlink identified that the categories of personal data affected by the Relevant Processing comprised special category data, and included data relating to criminal convictions and/or offences and genetic or biometric data.[74]

139. Birthlink also informed the Commissioner that the Linked Records may have contained handwritten letters from birth parents and birth families, photographs and other sensitive personal information.[75] Paragraph 72 of the Fining Guidance provides that the Commissioner may also consider private communications as being particularly sensitive (this is especially so when such communications contain intimate details or confidential information about an individual).

140. The Commissioner is satisfied that there is sufficient evidence to conclude that it is likely that highly sensitive personal data (including special category data) contained on some of the Linked Files was destroyed by the Relevant Processing. Some of the destroyed personal data is irreplaceable and its destruction is likely to have a detrimental impact on the affected data subjects. Examples of the impact likely to be caused to affected individuals is described at paragraphs 39 and 41 to 73 above.

141. As a consequence of the failure on the part of Birthlink to have in place appropriate data protection policies and procedures, including records of processing and retention and destruction policies, Birthlink has been

[74] Although the February 2025 Risk Assessment did not recognise the inclusion of data relating to criminal convictions/offences and genetic or biometric data, this was clarified at the Oral Representations Meeting. The sample files reviewed did not contain these categories of personal data. This is not sufficient to establish on the balance of probabilities that the Linked Files did not contain these categories of personal data or for the Commissioner to disregard the information contained in the Breach Report submitted by Birthlink dated 8 September 2023.
[75] Birthlink personal data breach report dated 8 September 2023 at p.3; Birthlink internal investigation report dated September 2023 at pp.1; 15

unable to identify how many data subjects have been impacted or which data subjects are likely to have had irreplaceable items destroyed. This increases the seriousness of the infringements.

Conclusion on seriousness of infringements

142. Having considered the nature, gravity and duration of the infringements, as well as their negligent character and the categories of personal data affected, the Commissioner categorises the infringements as having a high degree of seriousness.

143. In the absence of any mitigating factors, the infringements would warrant a monetary penalty.

Aggravating and mitigating factors

144. In determining the seriousness of Birthlink's infringements, the Commissioner must also consider whether any other factors aggravate or mitigate the position. The Commissioner has had regard to all the factors contained in Article 83(2) UK GDPR and addresses the provisions he considers are relevant in this case below.

Relevant aggravating or mitigating factors | Article 83(2)(c) any action taken by the controller or processor to mitigate the damage suffered by the data subjects

145. Birthlink told the Commissioner that it has no records of any measures taken to mitigate the detriment to data subjects immediately following the Relevant Processing.[76]

[76] Email from Birthlink to ICO dated 15 November 2023

146. Furthermore, it was only once the Care Inspectorate brought the personal data breach to the attention of the Interim Chief Executive Officer in September 2023 that Birthlink took any steps to review the impact of the Relevant Processing and improve its data protection compliance posture. These steps included:

    i. Completing an internal investigation and coming up with eight learning points and 14 recommendations. Birthlink has informed the Commissioner that the recommendations have since been implemented;

    ii. Implementing a data retention and data destruction policy;

    iii. Creating and maintaining a record of Birthlink's data processing activities;

    iv. Conducting data protection impact assessments in relation to its processing activities;

    v. Introducing mandatory data protection training for its staff (all staff had undertaken the training by 24 November 2023).

147. In its written representations, Birthlink gave the Commissioner further information on improvements to data protection and information governance which have been implemented. All incoming casework is now recorded digitally. Birthlink explained that:

"*The digitisation of the physical records began in June 2023 and is being undertaken concurrently with an audit of the Adoption Contact Register. This means that physical records are systematically being examined, and*

the physical record is being digitised and held electronically in the information management system. Quality assurance is built into the process to ensure that the data is reliably recorded".[77]

148. With regard to cherished or irreplaceable items, Birthlink told the Commissioner that there is now a box on the information management system to indicate there is a cherished item for the person and that cherished items are placed in archival preservation envelopes and filed in a fireproof, waterproof box.[78]

149. However, the Commissioner notes that the above steps were taken a significant period of time after the Relevant Processing occurred and are, in any event, unlikely to mitigate any damage caused to affected individuals.

150. Furthermore, the steps taken by Birthlink, after being notified of the personal data breach by the Care Inspectorate, are considered to be actions expected of any data controller in response to an incident of this nature.

151. The Commissioner has therefore been provided with no evidence that any steps have been taken to mitigate the potential impact of the personal data breach on data subjects.

152. Birthlink told the Commissioner that the risk to affected individuals is high. It recognises it is inevitable that those affected individuals' [redacted]

[77] Birthlink written representations 25 February 2025.
[78] Birthlink written representations 25 February 2025.

[redacted].[79]

153. Despite the high risk to the rights and freedoms of affected individuals recognised by Birthlink in September 2023, Birthlink has not communicated the personal data breach to affected individuals. Birthlink told the Commissioner that it has no record of what was destroyed and is reliant on individuals searching for information known to have been held on a Linked Record before it can determine if they have been affected.

154. Birthlink told the Commissioner that it conducted a risk assessment on whether to issue a public statement concerning the personal data breach. In deciding against issuing such a statement, Birthlink cited that it did not wish to cause unnecessary harm to its service users in leading them to believe that something significant had been destroyed when that may not have been the case.

155. The Commissioner considered whether it would be appropriate to make a finding of infringement of Article 34 UK GDPR[80] and to include consideration of this infringement in the decision to impose a penalty. The Commissioner decides that this would not be an appropriate or proportionate use of his powers. Birthlink has given some consideration to notifying data subjects and the Commissioner recognises the nuanced decision making required, in light of the concerns in respect of the wellbeing of data subjects.

[79] Birthlink internal investigation report dated September 2023 at p.14
[80] Article 34(1) UK GDPR: *When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*

156. The Commissioner next considered whether the failure on the part of Birthlink to notify impacted data subjects of the personal data breach and to take any steps to mitigate the damage suffered by data subjects, constitutes an aggravating factor.

157. In his provisional decision, the Commissioner was minded to conclude that this failure was an aggravating factor. However, in response to the notice of intent. Birthlink provided the Commissioner with detailed and considered representations on how it had assessed the appropriate ways it could have communicated the data breach to affected data subjects.[81]

158. After carefully considering these representations and noting the detail provided by Birthlink regarding the positive and negative impact of communicating the personal data breach to affected data subjects the Commissioner is no longer satisfied that this should be considered to be an aggravating factor. Whilst the Commissioner does not agree with the approach taken by Birthlink, he is satisfied that it was not motivated by attempts to avoid the financial implications of notifying data subjects. The main concern for Birthlink was the impact and outcomes for data subjects because it was not possible to identify how many data subjects were impacted or to identify who those data subjects were.

Relevant aggravating or mitigating factors | Article 83(2)(d) the degree of responsibility of the controller or processor

159. The Commissioner expects controllers processing personal data, regardless of their size or financial position (i.e. the resources available to it) to implement appropriate security measures and bear responsibility for, and demonstrate compliance with, the accountability principle.

[81] Birthlink written representations 25 February 2025

160. Birthlink was the sole controller in respect of the processing and was solely responsible for its own lack of awareness of, and compliance with, core principles of processing personal data. However, this factor has already been taken into account for the purposes of assessing Birthlink's substantive infringement of Article 5(2) UK GDPR.

Relevant aggravating or mitigating factors | Article 83(2)(f) the degree of cooperation with the Commissioner

161. The Commissioner acknowledges that Birthlink has co-operated with the investigation into the Relevant Processing. However, in doing so, Birthlink has not gone above and beyond the normal level of cooperation expected in response to a regulatory investigation.

162. In the circumstances, Birthlink's degree of cooperation is a neutral factor, which neither aggravates nor mitigates the infringements.

Relevant aggravating or mitigating factors | Article 83(2)(h) the manner in which the infringements became known to the Commissioner

163. Birthlink made a notification to the Commissioner in September 2023 (two years and five months after the Relevant Processing occurred). Whilst the Commissioner considers this to be a marked departure from the obligation on Birthlink to notify the Commissioner of a personal data breach within 72 hours, it has already been taken into account for the purposes of assessing Birthlink's substantive infringement of Article 33(1) UK GDPR.

164. Accordingly, the delay in notifying the Commissioner is not treated as an aggravating factor.

Relevant aggravating or mitigating factors | Article 83(2)(k) any other applicable aggravating or mitigating factors

165. For completeness, the Commissioner has considered whether there are any other relevant factors which operate to aggravate or mitigate the infringements.

166. No further aggravating or mitigating factors have been identified.

Conclusion on relevant aggravating and mitigating factors

167. There are no aggravating or mitigating factors which impact on the assessment of the seriousness of the infringements. The Commissioner therefore considers that a penalty remains appropriate.

Effectiveness, proportionality and dissuasiveness

168. The final stage involves a consideration of the effectiveness, proportionality and dissuasiveness of a penalty. The Commissioner considers the imposition of a penalty to be an effective, proportionate and dissuasive measure.

169. Imposing a penalty on Birthlink would promote compliance with data protection law and provide an appropriate sanction for the infringements.

170. A penalty will ensure Birthlink takes its data protection obligations seriously and takes appropriate steps to prevent personal data breaches in the future.

171. There is also a need to deter other organisations (including those in the same sector) that hold sensitive personal data from acting in the same way. The imposition of a penalty will also act as a deterrent to other organisations which might otherwise choose not to notify the Commissioner within 72 hours of becoming aware of a personal data breach.

172. Whilst the Commissioner has taken into account Birthlink's size and charitable status, given the seriousness of the infringements the Commissioner considers that the imposition of a penalty would nevertheless be proportionate. The penalty would not exceed what is considered to be appropriate and necessary in the circumstances to ensure compliance with data protection legislation and to provide an appropriate sanction for the infringements.

173. Birthlink submitted that in light of the financial pressures faced by Birthlink, the Commissioner should consider a reprimand so that "*the equivalent money and more can be spent to benefit past, current and future generations of service users*".[82]

174. The Commissioner has given careful consideration to this request and to the question of whether a reprimand would be appropriate in all the circumstances of this case. The Commissioner has had regard to the Fining Guidance and also to his Regulatory Action Policy[83]. Whilst a reprimand would allow the Commissioner to make a finding that Birthlink has infringed data protection legislation, for the reasons set out above it would not be an effective, proportionate or dissuasive response to the

[82] Birthlink written representations 25 February 2025
[83] https://ico.org.uk/media2/about-the-ico/documents/2259467/regulatory-action-policy.pdf

serious findings of infringement set out at paragraphs 86, 100 and 111 above.

Conclusion on decision on whether to impose a penalty

175. In light of the assessment above, the Commissioner decides to impose a penalty.

VI. Calculation of Penalty

176. The Fining Guidance sets out a five-step approach which the Commissioner proposes to apply to calculate the amount of a penalty:

Step 1 Assessment of the seriousness of the infringement.

Step 2 Accounting for turnover (where the controller or processor is part of an undertaking).

Step 3 Calculation of the starting point having regard to the seriousness of the infringement and, where relevant, the turnover of the undertaking.

Step 4 Adjustment to take into account any aggravating or mitigating factors.

Step 5 Assessment of whether the fine is effective, proportionate and dissuasive.

Following the application of this five-step approach, the Commissioner has gone on to consider the amount of the penalty.

Statutory maximum penalty

177. Article 83(3) UK GDPR states that "*if a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of the UK GDPR, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*".

178. The infringement of Article 5(1)(f) UK GDPR, which is a core principle for processing, is subject to the higher maximum statutory penalty of £17.5 million or 4% of worldwide turnover, whichever is higher (Article 83(5)(a) UK GDPR). Had the Commissioner imposed a separate penalty for each of the infringements, the total of those three penalties could not have exceeded £17.5 million.

179. However, for the reasons given in paragraph 116 above, the Commissioner has calculated a single penalty for all the infringements. The calculation proceeds on the basis of a single statutory maximum of £17.5 million.

A. Step 1 | Assessment of the seriousness of the infringement

180. As set out at paragraphs 109 to 115 of the Fining Guidance, the Commissioner determines a starting point for the penalty first by assessing the seriousness of the infringement. The Commissioner categorises the infringement according to its degree of seriousness and then chooses a starting point based on a percentage of the relevant applicable statutory maximum.

181. In this Penalty Notice, the Commissioner has categorised the infringements as having a high degree of seriousness. This means that

the starting point will be between 20% and 100% of the relevant legal maximum (£17.5 million).

182. The Commissioner decides that the infringements warrant a starting point of 70%.

183. A starting point of lower than 70% is not warranted due to the seriousness of the infringements. The highly sensitive and sentimental nature of some of the personal data, the absence of appropriate organisational measures to ensure the appropriate level of security for that data and the limited understanding of the core principles of data protection law support a starting point of 70%.

184. A starting point of higher than 70% is not warranted as the infringements were not intentional or committed for financial benefit and only some of the Linked Records were likely to have contained cherished or irreplaceable items.

B. Step 2 | Accounting for turnover

185. Having assessed the seriousness of the infringements, the Commissioner next determines any adjustment to reflect the size of the recipient of the penalty.[84] This is consistent with the need to ensure the amount of the penalty is effective, proportionate and dissuasive.

186. Where the recipient is an undertaking, the Commissioner will determine the adjustment by reference to the undertaking's turnover. As explained at paragraph 119 of the Fining Guidance, where a recipient is not an undertaking and therefore does not have turnover, the Commissioner

[84] As set out at paragraph 128 of the Fining Guidance, any such adjustment is discretionary.

may instead have regard to other indicators of the recipient's financial position, such as assets, funding or administrative budget.

187. Taking into account Birthlink's charitable status and the fact that the Relevant Processing in this case related to the provision of the Adoption Contact Register (which is not an economic activity), the Commissioner has determined that it is likely that Birthlink falls outside the definition of an undertaking. He has therefore adopted the more conservative approach of using Birthlink's support costs for the purpose of calculating the amount of the fine, rather than using the (higher) amount reflecting its total income (i.e. turnover). This is similar to the approach the Commissioner typically takes in relation to public authorities, where he has previously calculated the fine by reference to administrative budget.

188. In its Representations, Birthlink submitted that the provisional penalty had "*been calculated using the overall turnover rather than solely the post adoption service budget*".[85] This is not correct. As outlined above, the Commissioner calculated the penalty using Birthlink's support costs rather than overall turnover.

189. Birthlink provided the Commissioner with its financial statements for the year ended 31 March 2024.[86] Birthlink's support costs were £211,700 for the year ended 31 March 2024[87] and £211,316 for the year ended 31 March 2023.[88]

190. As set out in the Fining Guidance, in the case of a micro-enterprise with an annual turnover of up to £2 million, the Commissioner may apply an adjustment factor of between 0.2% and 0.4% to the starting point. In

[85] Birthlink written representations 25 February 2025
[86] Birthlink Financial Statements are published and audited: See F116_16_(Last accessed 11 June 2025)
[87] Birthlink Financial Statements Year Ended 31 March 2024 p.18
[88] Published online and accessible at: https://birthlink.org.uk/wp-content/uploads/2024/07/Birthlink_final_2023_accounts.docx.pdf [last accessed 11 June 2025]

light of the support costs reported by Birthlink, the Commissioner considers this range of adjustment to be appropriate for Birthlink's case.

191. The Fining Guidance sets out that the Commissioner is likely to choose a higher amount for undertakings with a higher turnover within the applicable range, these ranges are however only indicative. The Commissioner considers that in the circumstances of this case an adjustment of 0.3% is appropriate to reflect Birthlink's size and support costs as well as the need for the fine to be effective, proportionate and dissuasive.

C. Step 3 | Calculation of the starting point

192. The starting point of the penalty is calculated as follows:

Fixed statutory maximum (£17.5 million) x adjustment for seriousness (70%) x turnover adjustment (0.3%) = **£36,750** (thirty-six thousand seven hundred and fifty pounds)

D. Step 4 | Adjustment to take into account any aggravating or mitigating factors

193. The Commissioner next takes into account any aggravating or mitigating factors. These factors may warrant an increase or decrease in the level of the penalty calculated at the end of Step 3 (the starting point of £36,750).

194. the Commissioner decides not to make any adjustment to take into account the degree of responsibility of Birthlink. Any organisation regardless of size and financial position (ie the resources available to it) should be reasonably expected to implement appropriate security

measures to prevent the unauthorised destruction of records. However, as this factor has been taken into account already by the Commissioner, an increase in the level of the penalty is not warranted.

195. The Commissioner decides not to make any adjustment for aggravating or mitigating factors.

196. The amount determined at Step 4 is £36,750 = **£36,750** (thirty six thousand, seven hundred and fifty pounds).

E. Step 5: Adjustment to ensure the fine is effective, proportionate and dissuasive

197. As set out in the Fining Guidance *"the aim of Steps 1 to 4 of the calculation is to identify a fine amount that is effective, proportionate and dissuasive. The purpose of Step 5 is to provide the opportunity for the Commissioner to check that is the case"*.

198. The Commissioner considers that a penalty of £36,750 will be effective, proportionate and dissuasive. It is an appropriate sanction for the infringements which have been found and is therefore effective.

199. A penalty in this amount will be dissuasive. It will have a genuine deterrent effect, taking into account both the specific deterrent to Birthlink and the general deterrence to other small organisations providing this type of service

200. Taking into account Birthlink's size and charitable status and the very serious nature of the infringements, the penalty is proportionate.

201. In making his decision and setting the amount of the penalty, the Commissioner has also had regard to the desirability of promoting economic growth (as required by section 108(1) of the Deregulation Act 2015). In particular, the Commissioner has taken into consideration:

a. the nature and level of risk associated with non-compliance with data protection legislation (including risks to economic growth);

b. the steps taken by Birthlink to achieve compliance and the reasons for its failure;

c. the willingness and ability of Birthlink to address its non-compliance;

d. the likely impact of the proposed intervention on Birthlink and the likely impact of the Commissioner's regulatory intervention (both in terms of deterrence and economic benefits to legitimate businesses).

202. Having regard to the factors stated above, the Commissioner considers that this Penalty Notice is unlikely to have an impact on any measure of economic activity or growth in the United Kingdom, including levels of employment and Gross Domestic Product.

F. Financial hardship

203. Paragraph 151 of the Fining Guidance outlines that, in exceptional circumstances, the Commissioner may reduce a fine where an organisation is unable to pay due to its financial position.

204. In response to the notice of intent, Birthlink provided representations to the Commissioner that:

a. A fine would impact mainly on people seeking services from Birthlink and will delay organisation improvement, where financial investment is critically needed;

b. [redacted];

c. [redacted];

d. [redacted];

e. The funds held by Birthlink for other projects are restricted and cannot be used to pay the penalty.[89]

205. In addition to these points, in oral representations on financial hardship, Birthlink submitted that:

[redacted]

[89] Birthlink written representations 25 February 2025

[redacted]

e. Birthlink's written submissions outlined the investments which had been made on infrastructure to ensure Birthlink is in a better position to deal with information governance and data protection moving forward. [redacted].[90] A monetary penalty will have an impact on this investment.

206. As explained at paragraph 152 of the Fining Guidance, "*The Commissioner will only grant a reduction for financial hardship on the basis of objective evidence that imposing the proposed fine would irretrievably jeopardise an organisation's economic viability… The Commissioner will not base any reduction on the mere finding of an adverse … financial situation*."

[90] Minutes of oral representations meeting 19 March 2025

207. The Commissioner finds that the representations from Birthlink go beyond the confines of a mere adverse financial situation. Birthlink has submitted with sufficient clarity details of the exceptional financial challenges which Birthlink faces.

208. While the Commissioner has given careful consideration to the representations made on financial hardship, he finds that Birthlink should not avoid a penalty solely on the basis of its financial position, given the serious nature of the infringements.

209. A claim for financial hardship will only justify a reduction in the penalty in exceptional circumstances. However, the Commissioner considers that a further reduction in the amount of the penalty is both proportionate and necessary in order to avoid the risk to Birthlink's financial sustainability in the exceptional circumstances outlined above. In these circumstances, a reduction in the penalty is required to avoid irretrievably jeopardising the services provided by Birthlink.

210. The Commissioner has taken into account enforcement action on previous cases and applied his skill and judgement to assess the appropriate level of reduction. The Commissioner is satisfied that a reduction to a penalty of £18,000 will appropriately reflect the representations from Birthlink on financial hardship whilst ensuring the penalty is effective, dissuasive and proportionate.

G. Conclusion- Penalty

211. For the reasons set out above, the Commissioner has decided to impose an administrative penalty on Birthlink in the amount of **£18,000.**

VII. PAYMENT OF THE PENALTY

212. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by 23 July 2025 at the latest.

213. The penalty is recoverable by Order of the County Court or the High Court.

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

- the period within which a penalty must be paid has expired and all or any of the penalty has not been paid;
- all relevant appeals against the penalty and any variation of it have either been decided or withdrawn; and
- the period for appealing against the penalty and any variation of it has expired.

VIII. RIGHTS OF APPEAL

215. By virtue of section 162 DPA, Birthlink may appeal to the First-tier Tribunal (General Regulatory Chamber) (Information Rights) against this Penalty Notice. Birthlink may appeal to the Tribunal against the amount of the penalty, whether or not Birthlink appeals against the Penalty Notice.

216. Information about the appeals process is set out in Annex 1. Any notice of appeal should be sent or delivered to the Tribunal so that it is received within 28 days of the date of this Penalty Notice.

Dated the 24 day of June 2025

Sally Anne Poole
Head of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

DATA PROTECTION ACT 2018

RIGHTS OF APPEAL

1. By virtue of section 162(1) of the DPA, you may appeal to the Tribunal against this Penalty Notice. By virtue of section 162(3), you may appeal to the Tribunal against the amount of the penalty specified in this Penalty Notice, whether or not you appeal against this Penalty Notice.

2. If you appeal and if the Tribunal considers: a. that the notice or decision against which the appeal is brought is not in accordance with the law; or b. to the extent that the notice or decision involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently, the Tribunal must allow the appeal or substitute another notice or decision which the Commissioner could have given or made.

3. You may bring an appeal by sending a notice of appeal to the Tribunal at: grc@justice.gov.uk or

General Regulatory Chamber

PO Box 11230

Leicester

LE1 8FQ

(Telephone: 0300 123 4504)

a. The notice of appeal should be received by the Tribunal within 28 days of the date of this Penalty Notice (which is the date that this Penalty Notice was sent).

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

4. The notice of appeal must include:

a. your name and address;

b. the name and address of your representative (if any);

c. an address where documents may be sent or delivered to you;

d. the name and address of the respondent (the Information Commissioner);

e. details of the decision to which the proceedings relate;

f. the result you are seeking;

g. the grounds on which you rely;

h. a full copy of this Penalty Notice; and

i. (if the notice of appeal is late) a request for an extension of time, giving the reason(s) why the notice of appeal is late and why the Tribunal should accept it.

5. 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 their case themselves or may be represented by any person whom they may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and The Tribunal For Public Release 55 Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20))

ANNEX 2

LEGAL FRAMEWORK

1. Section 155 DPA provides that, if the Commissioner is satisfied that a person has failed, or is failing, as described in section 149(2) DPA, the Commissioner may, by written penalty notice, require the person to pay to the Commissioner an amount in sterling specified in the penalty notice.

2. The types of failure described in section 149(2) DPA include:

    a) **Section 149(2)(a)** | "*where a controller or processor has failed, or is failing, to comply with… a provision of Chapter II of the UK GDPR… (principles of processing)*"; and

    b) **Section 149(2)(c)** | "*where a controller or processor has failed, or is failing, to comply with… a provision of Articles 25 to 39 of the UK GDPR… (obligations of controllers and processors)*".

Principles of processing

3. Chapter II UK GDPR sets out the principles relating to the processing of personal data which controllers must comply with. Article 5 UK GDPR sets out the principles relating to processing of personal data.

4. The principles of processing relevant to this Penalty Notice include:

    a) **Article 5(1)(a)** | "*personal data shall be… processed lawfully, fairly and in a transparent manner in relation to the data*

subject" (the '**lawfulness, fairness and transparency**' principle).

b) **Article 5(1)(e)** | *"personal data shall be… kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed…"* (the '**storage limitation**' principle);

c) **Article 5(1)(f)** | *"personal data shall be… processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*" (the '**integrity and confidentiality**' principle).

d) **Article 5(2)** | "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1" (the '**accountability'** principle).

Obligations on controllers and processors

5. Chapter IV of the UK GDPR sets out the obligations of controllers and processors under the data protection regime. The obligations relevant to this Penalty Notice include:

a) Article 32 (security of processing)

"(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and

organisational measures to ensure a level of security appropriate to the risk…

(2) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

b) Article 33 (Notification of a personal data breach to the Commissioner)

"(1) In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay."

6. The Commissioner has also had regard to the following defined terms as provided by Article 4 UK GDPR, which are material to this Penalty Notice:

a) Article 4(1) ('personal data')

"means any information relating to an identified or identifiable natural person".

b) Article 4(2) ('processing')

"means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

c) Article 4(6) ('filing system')

"means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis".

d) Article 4(7) ('controller')

"means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data…"

e) Article 4(12) ('personal data breach')

"means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

7. The above provides the relevant legal framework for the purpose of this Penalty Notice. The body of the Penalty Notice may include other legal provisions which were relevant to the Commissioner's determination to impose a financial penalty.