

DATA PROTECTION ACT 2018 (PART 6, SECTION 155)

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

TO: The Central Young Men's Christian Association ("the Central YMCA")

OF: 112 Great Russell Street, London WC1B 3NQ.

Introduction and Summary

1. The Information Commissioner ("the Commissioner") has decided to issue the Central YMCA with a monetary penalty under section 155 of the Data Protection Act 2018 ("the DPA"). The penalty notice imposes an administrative fine on the Central YMCA, in accordance with the Commissioner's powers under Article 83 of the General Data Protection Regulation 2016 (the "UK GDPR"). The amount of the penalty is £7,500 (seven thousand five hundred pounds).
2. The penalty is in relation to contraventions of Articles 5(1)(f) and 32(1) and (2) of the UK GDPR and an incident on 6 October 2022 (the "relevant date") affecting personal data processed by the Central YMCA on the relevant date.
3. For the reasons set out in this Monetary Penalty Notice, the Commissioner has found that the Central YMCA failed to ensure appropriate security of

personal data in its control by implementing appropriate technical and organisational measures and appropriate policies and procedures, as required by Article 5(1)(f) and Article 32(1) of the UK GDPR.

4. This Monetary Penalty Notice explains the Commissioner's decision, including the Commissioner's reasons for issuing the penalty and for the amount of the penalty. The Central YMCA has had an opportunity to make representations to the Commissioner in response to the Notice of Intent regarding this penalty. Instead of making representations the Central YMCA has decided to accept the Notice of Intent and the Commissioner's findings.

Legal Framework

Obligations of the Controller

5. The Central YMCA is a controller for the purposes of the UK GDPR and the DPA, because it determines the purposes and means of processing of personal data (UK GDPR Article 4(7)).
6. "Personal data" is defined by Article 4(1) of the UK GDPR to mean:

"information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

7. "Processing" is defined by Article 4(2) of the UK GDPR to mean:

"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"

8. Article 9 of the UK GDPR prohibits the processing of "special categories of personal data" unless certain conditions are met. The special categories of personal data subject to Article 9 include:

"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, bio-metric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

9. Controllers are subject to various obligations in relation to the processing of personal data, as set out in the UK GDPR and the DPA. They are obliged by Article 5(2) to adhere to the data processing principles set out in Article 5(1) of the UK GDPR. Article 5(2) makes clear that the "controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".
10. In particular, controllers are required to implement appropriate technical and organisational measures to ensure that their processing of personal

data is secure, and to enable them to demonstrate that their processing is secure. Article 5(1)(f) ("Integrity and Confidentiality") stipulates that:

"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".

11. Article 32 of the UK GDPR also provides that:

"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, including inter alia as appropriate:

- (a) the pseudonymisation and encryption of personal data;*
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

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."

The Commissioner's Powers of Enforcement

12. The Commissioner is the supervisory authority for the UK, as provided for by Article 51 of the UK GDPR.
13. By Article 57(1) of the UK GDPR, it is the Commissioner's task to monitor and enforce the application of the UK GDPR.
14. By Article 58(2)(d) of the UK GDPR the Commissioner has the power to notify controllers of alleged infringements of the UK GDPR. By Article 58(2)(i) he has the power to impose an administrative fine, in accordance with Article 83, in addition to or instead of the other corrective measures referred to in Article 58(2), depending on the circumstances of each individual case.
15. By Article 83(1), the Commissioner is required to ensure that administrative fines issued in accordance with Article 83 are effective, proportionate, and dissuasive in each individual case. Article 83(2) goes on to provide that:

"When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(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 supervisory authority, 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 supervisory authority, 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.”

16. Article 83(5) UK GDPR provides, inter alia, that infringements of the obligations imposed by Article 5 UK GDPR on the controller and processor will, in accordance with Article 83(2), be subject to administrative fines of up to €20 million or, in the case of an undertaking, up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher.
17. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner.¹ Section 155 of the DPA sets out the matters to which the Commissioner must have regard when deciding whether to issue a penalty notice and when determining the amount of the penalty and provides that:

¹ Section 115 DPA establishes that the Commissioner is the UK's supervisory authority for the purposes of the UK GDPR.

"(1) If the Commissioner is satisfied that a person—

(a) has failed or is failing as described in section 149(2) ...,

the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.

(2) Subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the following, so far as relevant—

(a) to the extent that the notice concerns a matter to which the GDPR applies, the matters listed in Article 83(1) and (2) of the UK GDPR."

18. The failures identified in section 149(2) DPA are, insofar as relevant here:

"(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—

(a) a provision of Chapter II of the UK GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);

...;

(c) a provision of Articles 25 to 39 of the UK GDPR or section 64 or 65 of this Act (obligations of controllers and processors) [...]”

19. Schedule 16 includes provisions relevant to the imposition of penalties. Paragraph 2 makes provision for the issuing of notices of intent to impose a penalty, as follows:

“(1) Before giving a person a penalty notice, the Commissioner must, by written notice (a “notice of intent”) inform the person that the Commissioner intends to give a penalty notice.”

The Commissioner's Regulatory Action Policy

20. Pursuant to section 160(1) DPA, the Commissioner published his Regulatory Action Policy (“RAP”) on 7 November 2018.
21. The process the Commissioner will follow in deciding the appropriate amount of a penalty to be imposed is described in the RAP from page 27 onwards. In particular, the RAP sets out the following five-step process:
- a. Step 1. An ‘initial element’ removing any financial gain from the breach.
 - b. Step 2. Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2) - (4) DPA.

- c. Step 3. Adding in an element to reflect any aggravating factors. A list of aggravating factors which the Commissioner would take into account, where relevant, is provided at page 11 of the RAP. This list is intended to be indicative, not exhaustive.
- d. Step 4. Adding in an amount for deterrent effect to others.
- e. Step 5. Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship). A list of mitigating factors which the Commissioner would take into account, where relevant, is provided at page 11-12 of the RAP. This list is intended to be indicative, not exhaustive.

Circumstances of the Failure: Facts

General Background

- 22. This Penalty Notice does not purport to identify exhaustively each and every circumstance and document relevant to the Commissioner's investigation. The circumstances and documents identified below are a proportionate summary.
- 23. The Central YMCA is an education and wellbeing charity registered as a data controller with the Information Commissioner's Office (the "ICO"). It provides a number of community programmes, one of which is the Positive Health Programme.

24. The Positive Health Programme ("Programme") is run by the Positive Health team as part of YMCA Club. YMCA Club is a large gym facility, which is part of the Central YMCA.
25. The Programme is an exercise scheme for people living with HIV. As part of the Programme, the Central YMCA collects special category data (the aims of referral to the Programme, the date of HIV diagnosis, the medication taken, the individual's medical statistics, other medical history and their referring clinician/hospital).
26. On 6 October 2022 at approximately 15:34 BST, a co-ordinator for the Programme sent an email to a mailing list of 270 recipients, inviting them to a talk about nutrition.
27. The Programme co-ordinator used an email programme (Microsoft Outlook) to send the email. At the relevant date, the Central YMCA had a verbally communicated policy that the Programme team should send event invitations via Microsoft Outlook using the blind carbon copy ("BCC") function.
28. The co-ordinator unfortunately included those email addresses in the carbon copy ("CC") function, thus revealing all of the email addresses to all 270 recipients.
29. The day after, on realising the error, the co-ordinator used the recall function within Microsoft Outlook to try and recall the email sent. This however led to another email to all 270 recipients. It was the Programme team's belief that this would remove the original message from the recipients' inboxes.

The number of data subjects involved

30. Whilst the emails had been sent to 270 recipients, there were duplicates, so they were sent to 264 unique email addresses.
31. The emails were not delivered to 9 of those email addresses, so the emails were delivered to 255 recipients, disclosing 264 email addresses.
32. The Central YMCA then assessed that 115 of those had clear names in them, and a further 51 contained at least part of a name, making them potentially identifiable. Therefore 166 data subjects were affected by the breach, all of whom are in the Programme.

The nature of the personal data and special category data disclosed

33. As part of its guidance and resources relating to UK GDPR, the Commissioner has produced detailed guidance in relation to special category data. The guidance includes a sub-section titled 'What is special category data?' which establishes that special category data is not just personal data which specifies relevant details but also personal data "revealing or concerning" those details. The test to be met is whether the relevant information can be inferred with a reasonable degree of certainty, and if so, it is likely to be special category data.
34. As well as the disclosure of 166 email addresses containing personal data, the context of the email was the Programme. The invite to the event for nutrition guidance to individuals meant that it can be reasonably assumed that the recipients of the email would be aware that the Programme is directed at individuals with HIV. If the recipients were not part of the

Programme, they could find out what the Programme was on the Central YMCA's website.

35. Recipients of the email can therefore infer from its contents that the 166 individuals whose email addresses were disclosed in the breach were likely to be living with HIV, meaning that the disclosed personal data included health data, which in turn is special category data under Article 9(1) of the UK GDPR.
36. The Central YMCA had also set expectations of privacy in its Programme, and that some members of the Programme may have wished to remain anonymous, even to other members of the Programme, whilst noting that "all recipients are assumed to have an HIV positive diagnosis".
37. Even if the personal data was not considered to be special category data, there are particular sensitivities regarding the personal data being processed in the Programme, which the Central YMCA should have considered and taken a cautious approach when processing it, as set out in the Commissioner's guidance referred to in paragraph 33:

"If you think the data carries a risk of inferences that might be considered sensitive or private, even if this falls short of revealing something about one of the special categories with any level of certainty, then you should also carefully consider fairness issues and whether there is anything more you can do to minimise privacy risks."

Discovery of the breach, reporting to the Commissioner and communications to data subjects

38. The Central YMCA became aware of the breach on the morning after the email was sent, as a result of complaints received from recipients.
39. The YMCA Club informed the Central YMCA's Data Protection Officer (DPO) later that morning, with a breach report being made to the ICO that evening. This was in line with Article 33 of the UK GDPR and within the 72 hour period.
40. In accordance with Article 34 of the UK GDPR the Central YMCA notified affected data subjects on 10 October 2022, setting out the cause of the breach, took accountability for the error and informed data subjects of the steps the Central YMCA were taking, including reporting the incident to the ICO and conducting an internal review. The data controller provided the DPO's contact details for anyone affected to ask questions or to discuss how the breach had affected them.

The Commissioner's Investigation

41. The Commissioner first wrote to the Central YMCA on 14 December 2022 asking for further information in relation to the actions the Central YMCA had taken following the data breach notification it had made on 7 October 2022. During the period between February 2023 and April 2023, subsequent enquiries were raised by the Commissioner seeking additional information from the Central YMCA.
42. The Commissioner's investigation found four key areas where the Central YMCA failed to take reasonable steps to prevent this breach:
 - a. The Central YMCA had no written policy in place regarding the sending of group emails,

- b. The Central YMCA had access to an email marketing platform (and the use of this platform would have reduced the likelihood of an inappropriate disclosure) however the Central YMCA did not use it in this case,
- c. The Central YMCA failed to effectively monitor completion of data protection training, and
- d. There is evidence of deficiencies within the Central YMCA's data protection training.

The Contraventions of Articles of 5 (1)(f) and 32 (1) and (2) of the UK GDPR

- 43. The Commissioner has considered whether the facts set out above constitute a contravention of the data protection legislation.
- 44. For the reasons set out below, the Commissioner has taken the view from his investigation that this breach occurred as a result of serious deficiencies in the technical and organisational measures implemented by the Central YMCA.
- 45. For the reasons set out below, and having carefully considered the information provided by the Central YMCA, the Commissioner's view is that the Central YMCA failed to comply with Articles 5 (1)(f) and 32(1) and (2) of the UK GDPR.

Article 5 (1)(f) and 32(1) and (2) of the UK GDPR

46. The Commissioner finds that the Central YMCA has failed to comply with the requirements of Article 5(1)(f) of the UK GDPR, including to process personal data *"in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing, using appropriate technical or organisational measures"*. In making this determination, the Commissioner takes into account the Central YMCA's failure to comply with Articles 32(1), 32(1)(a), 32(1)(b) and 32(2) of the UK GDPR, which was demonstrated by the Central YMCA's failure to implement appropriate technical and organisational measures:

- a. not having a relevant written policy or procedure in place;
- b. inappropriately relying on the use of BCC to send group emails;
- c. not providing data protection training specific to employee roles and levels of access to personal data;
- d. a lack of awareness of data protection legislation within some parts of the organisation; and
- e. not effectively monitoring completion of data protection training.

(1) not having a relevant written policy or procedure

47. At the time of the security incident, the Central YMCA did not have sufficient written information security policies or procedures to prevent this breach. It only had a verbal policy to use BCC in emails, both of which are insufficient and not appropriate for managing special category data. It also communicated relatively frequently using this method.

48. Another part of the Central YMCA (the Communications and Marketing team) had an email marketing tool, BrotherMailer, which could have been used to mitigate this risk and handle the special category data

appropriately, by sending individual emails to each recipient. However, the Central YMCA did not know that the Programme was sending emails of this nature.

49. Relevant industry standards and guidance, including ISO27001, NIST Cyber Security Framework, and the ICO and National Cyber Security Centre co-published guidance, "GDPR Security Outcomes", establish that organisations should have written security policies and procedures in place.
50. ISO27001 recommends that: *"A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties"*. The NIST Cyber Security Framework requires that an: *"Organizational cybersecurity policy is established and communicated"*, and the GDPR Security Outcomes sets out that to protect personal data against cyber-attacks organisations should *"define, implement, communicate and enforce appropriate policies and processes that direct your overall approach to securing systems involved in the processing of personal data"*.
51. It is the Commissioner's view that the lack of documented and appropriate security policies and procedures to deal with the sending of emails with special category data was in non-compliance with Article 32(1) of the UK GDPR. The lack of such documentation also contributed to the Central YMCA failing to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing, using appropriate technical or organisational measures, as required by Article 5(1)(f) of the UK GDPR. It also meant that the Central YMCA had not assessed the appropriate

level of security with regard to the risks of its data processing, particularly here in respect of the unauthorised disclosure of an individual's special category data to other participants in the Programme, as required by Article 32(2) of the UK GDPR.

(2) inappropriately relying on the use of BCC to send group emails

52. As the Commissioner refers to above, the lack of a documented policy meant that whilst the Programme co-ordinator believed that they were acting in an appropriate way, following the verbal policy to use BCC, this was an inappropriately insecure method of doing so. This is because it relies on the individual sending the email to ensure that it goes in the BCC field and not, as happened here, in the CC field, thus exposing individuals' special category data.
53. The Central YMCA had the financial and organisational means to implement BrotherMailer in the Programme team but failed to do so. As the Central YMCA procured the BrotherMailer tool for use elsewhere in the Central YMCA, it can be inferred that parts of the Central YMCA knew that reliance on sending emails by BCC was inappropriate, but that this knowledge, the process and the tool were not appropriately communicated throughout the Central YMCA.
54. If the Central YMCA had used BrotherMailer it would also have likely safeguarded the personal data from inappropriate disclosure.

(3) not providing data protection training specific to employee roles and levels of access to personal data

55. The Central YMCA told the Commissioner that the Programme co-ordinator had been initially a self-employed contractor in a different team. They had not completed data protection training and it had been the Central YMCA's policy to provide training only to employees.
56. This changed in March 2022, but as the Commissioner notes below in point 5, the Programme co-ordinator still did not take the training.
57. The Central YMCA used a training partner called Bob's Business Ltd. The Central YMCA provided copies of this training to the Commissioner during the investigation. It included sections on the sending of group emails, but it also stated (despite what the Central YMCA said about there being no written policy) that individuals should use BCC when sending to multiple contacts.
58. Whilst completion of that training may have reduced the risk of the inappropriate disclosure, BCC is still a high risk method of sending emails and hence the training would not have eliminated the risk of human error.
59. The training did not highlight the increased risks when processing special category data, nor did it bring attendees' attention to the fact that there was within the Central YMCA the BrotherMailer platform available which would have provided an appropriately secure alternative method to send emails.
60. The Commissioner expected the Central YMCA to provide role specific data protection training, at a sufficient quality to ensure that data protection is understood, and proportionate to the individual's level of access to, and sensitivity of, personal data.

(4) a lack of awareness of data protection legislation within some parts of the organisation

61. The Commissioner noted in its investigation that there is evidence of a lack of awareness of data protection legislation in the Programme team. For example, they did not initially understand the seriousness of the breach, referring to a "possible breach" when reporting it, and stating that the email "contained no private information".

(5) not effectively monitoring completion of data protection training

62. The Programme co-ordinator had not completed data protection training prior to the data breach. At the relevant time, 73% of workers at the Central YMCA had completed the relevant training module.
63. Before the Programme co-ordinator moved to a fixed term contract in 2022, they were signed up to certain induction modules, including data protection training. They did not complete this training, nor did they do so when training was required for self-employed contractors. A process was in place for line managers to ensure induction checklists were completed, but there was no central oversight. A reporting mechanism was in place to assess non-completion, but this did not work either.
64. The Commissioner expected the Central YMCA to monitor training effectively and ensure that mandatory training was completed, in line with the Central YMCA's policies.

Factors relevant to whether a penalty is appropriate, and if so, the amount of the penalty

65. The Commissioner has considered the factors set out in Article 83(2) of the UK GDPR in deciding whether to issue a penalty. For the reasons given below, he is satisfied that: (i) the contraventions are sufficiently serious to justify issuing a penalty in addition to exercising his corrective powers; and (ii) the contraventions are serious enough to justify a significant fine.

(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

Nature:

66. As the Commissioner sets out above, this was a disclosure of special category data in circumstances where confidentiality was expected, and the Central YMCA had not taken appropriate actions to appropriately secure the special category data. The Central YMCA had intended to use BCC which is not appropriately secure, and the Programme co-ordinator then used CC which was not secure.

67. The Commissioner's investigation into the incident revealed multiple infringements of the UK GDPR as set out in paragraphs 41 to 64 above. In particular, the Commissioner found breaches of Article 5(1)(f) and 32(1) and (2) due to: no written policy being in place for the sending of group emails; the email marketing platform not being used hence CC being used by mistake; not effectively monitoring the completion of data protection training; and deficiencies within that training itself.

Gravity:

68. The contravention is serious, in particular having regard to the sensitivity of the personal data processed by the Central YMCA.
69. In addition, the Commissioner takes account of the risks to data subjects that arise from the loss of control and disclosure of what they considered and expected to be confidential special category data, as it was special category data for 166 data subjects given that a positive HIV diagnosis can be inferred with a reasonable degree of certainty.

Number of data subjects

70. The number of data subjects is 166, as set out above at paragraph 69.

Duration

71. The Commissioner considers that the contraventions relating to Articles 5(1)(f) and 32(1) of the UK GDPR were from 6 October 2022 at 15:34 BST when the breach occurred. It was not until 10 October 2022 that the individuals on the affected mailing list were emailed to advise of the breach.

(b) the intentional or negligent character of the infringement

72. The Commissioner considers that the infringement was negligent for the reasons set out in paragraphs 66 to 69 above.

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

73. The Central YMCA complied with Article 34 of the UK GDPR to notify data subjects of the personal data breach, but this took from 6 October to 10 October to do so.
74. The Central YMCA also implemented short and longer term remedial measures, including an attempted email recall which was ineffective, immediate breach reporting to the Central YMCA DPO and feedback to the staff involved about the approach they had taken being ineffective.

(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

75. Article 32 of the UK GDPR requires organisations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by their processing; to include the potential impacts these risks may have on the rights and freedoms of natural persons.
76. More specifically, Article 32(1)(b) of the UK GDPR requires organisations to implement measures that ensure the ongoing confidentiality, integrity, availability and resilience of their processing systems and services.
77. The Commissioner is satisfied that for the reasons set out in the paragraphs above that the Central YMCA did not have sufficient measures

in place to ensure the ongoing integrity and resilience of processing systems and services in line with Articles 5(1)(f) and 32(1).

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

78. The Commissioner has not identified any relevant previous infringements by the Central YMCA.

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

79. The Central YMCA fully cooperated with the Commissioner's investigation.

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

80. The categories of personal data affected is set out above at paragraphs 33 to 37.

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

81. The Central YMCA self-reported the personal data breach to the Commissioner within 72 hours of becoming aware of the incident.

(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;

82. Not applicable.

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

83. Not applicable.

(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.

84. The Commissioner has considered the following **aggravating factors** in this case:

a. Not applicable.

85. The Commissioner took into account the following **mitigating factors**:

a. Not applicable.

Summary and Penalty

86. For the reasons set out above, the Commissioner has decided to impose a financial penalty on the Central YMCA. Taken together the findings above concerning the infringement, its likely impact, and the fact that the Central YMCA failed to comply with its GDPR obligations, the Commissioner has decided to apply an effective, dissuasive and proportionate penalty reflecting the seriousness of the breach which has occurred.

Calculation of Penalty

87. The Commissioner considers that imposition of a financial penalty would be an effective and proportionate action to ensure future compliance.
88. Following the Five Step process set out in the RAP the calculation of the proposed penalty is as follows.
89. Step 1: An initial element removing any financial gain from the breach. There was no evidence of financial gain from the breach.
90. Step 2: Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) DPA. This refers to and repeats the matters listed in Article 83(1) and (2) as set out above. The details are set out above and the conclusion at step 2, taking into account: (a) the matters set out above at paragraphs 65 to 83, (b) the matters referred to in this section and (c) the need to apply an effective proportionate and dissuasive fine the Commissioner considers that a penalty of £300,000 would be appropriate before adjustment in accordance with Steps 3-5 below. This amount is considered appropriate to reflect the seriousness of the breach and takes into account in particular the need for the penalty to be effective, proportionate and dissuasive.
91. Step 3: Adding in an element to reflect and aggravating factors (Article 83(2)(k)). The Commissioner considered that there were no additional factors relevant to the setting of the penalty were addressed during Step 2.

92. Step 4: Adding an amount for deterrent effect to others. The Commissioner considered that the factors relevant to the setting of the penalty were addressed during Step 2.
93. Step 5: Reducing the amount to reflect any mitigating factors including ability to pay. The Commissioner does not believe that there are any mitigating factors relevant to step 5 even though new procedures have been implemented and better training and written policies have been applied. The Commissioner expects any organisation to have these in place as a matter of course. However, taking into account the Commissioner's current policy and its action on previous cases, the Commissioner reduced the value of the fine to £7,500.

The amount of the penalty

94. For the reasons explained above, the Commissioner is satisfied that the conditions from the factors set out in Article 83(2) of the UK GDPR have been met in this case and that he has adopted fair procedure. The latter has included issuing a Notice of Intent, in which the Commissioner set out his preliminary thinking. The Central YMCA had the opportunity to make written representations in response to the Notice of Intent but instead has decided to accept the Notice of Intent and the Commissioner's findings.
95. In making his decision, the Commissioner has also had regard to the factors set out in s108(2)(b) of the Deregulation Act 2015; including: the nature and level of risks associated with non-compliance, including the risks to economic growth; the steps taken by the business to achieve compliance and reasons for its failure; the willingness and ability of the business to address non-compliance; the likely impact of the proposed

intervention on the business, and the likely impact of the proposed intervention on the wider business community, both in terms of deterring non-compliance and economic benefits to legitimate businesses.

96. Taking into account all of the factors set out above, the Commissioner has decided to impose a penalty on the Central YMCA of **£7,500 (seven thousand and five hundred pounds)**.

Conclusion

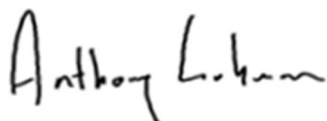
97. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **3 April 2024** at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.
98. There is a right of appeal to the First-tier Tribunal (Information Rights) against:
- a) The imposition of the penalty; and/or,
 - b) The amount of the penalty specified in the penalty notice
99. Any notice of appeal should be received by the Tribunal within 28 days of the date of this penalty notice.
100. The Commissioner will not take action to enforce a penalty unless:
- the period specified within the notice 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 notice 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

101. In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

102. Your attention is drawn to Annex 1 to this Notice, which sets out details of your rights of appeal under s.162 DPA 2018.

Dated the 6th day of March 2024



Anthony Luhman
Temporary Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

Rights of appeal against decisions of the Commissioner

1. Section 162 of the Data Protection Act 2018 gives any person upon whom a penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-
 - a) that the notice against which the appeal is brought is not in accordance with the law; or

 - b) to the extent that the notice involved an exercise of discretion by the Commissioner, that she ought to have exercised her discretion differently

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

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

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

Telephone: 0203 936 8963
Email: grc@justice.gov.uk

- a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.
- b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

- a) your name and address/name and address of your representative (if any);
- b) an address where documents may be sent or delivered to you;
- c) the name and address of the Information Commissioner;
- d) details of the decision to which the proceedings relate;
- e) the result that you are seeking;
- f) the grounds on which you rely;
- g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;
- h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

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 his case himself or may be represented by any person whom he 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 Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).