

# DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

## REPRIMAND

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

**OF:** 112 Great Russell Steet, London WC1B 3NQ.

1.1 The Information Commissioner ("the Commissioner") issues a reprimand to the Central YMCA in accordance with Article 58(2)(b) of the UK General Data Protection Regulation ("UK GDPR") in respect of certain infringements of the UK GDPR.

### The reprimand

1.2 The Commissioner has decided to issue a reprimand to the Central YMCA in respect of the following infringements of the UK GDPR:

- **Article 5(1)(f)** which states:

*"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 ('integrity and confidentiality')."*

- **Article 32(1) and (2)** which state:

*"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."*

1.3 The reasons for the Commissioner's findings are set out below.

1.4 The Central YMCA is an education and wellbeing charity that provides a number of community programmes, including the Positive Health Programme. The Positive Health Programme ("Programme") is an exercise scheme for people living with HIV and is run by the Positive Health Team as part of YMCA Club.

1.5 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. The co-ordinator included the recipients' email addresses in the carbon copy ("CC") function, thus revealing all of the email addresses to all 270 recipients. The day after, the co-ordinator used the recall function, which led to another email to all 270 recipients.

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

1.7 With a reasonable degree of certainty, recipients of the email can infer from its contents that the 166 individuals, whose email addresses were disclosed in the breach, were likely to be living with HIV. This means that the disclosed personal data included health data, which is special category data under Article 9(1) of the UK GDPR.

**Article 5(1)(f) and Article 32(1) and (2):**

1.8 The Commissioner considers that the Central YMCA failed to ensure appropriate security of personal data and failed to implement technical and organisational security measures appropriate to the risk of the processing.

1.9 At the time of the incident, the Central YMCA did not have sufficient

written information security policies and procedures to prevent this breach. It only had a verbal policy to use blind carbon copy ("BCC") in emails, both of which is insufficient and not appropriate for managing special category data.

1.10 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. The Central YMCA had the financial and organisational means to implement BrotherMailer in the Programme team, but failed to do so. If the Central YMCA had used BrotherMailer, it would have likely safeguarded the personal data from inappropriate disclosure.

1.11 The Central YMCA failed 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 the sensitivity of, personal data. The Commissioner noted there is evidence of a lack of awareness of data protection legislation in the Programme team.

1.12 The Programme co-ordinator had not completed data protection training prior to the breach. The Commissioner found that the Central YMCA had failed to monitor training effectively and ensure that mandatory training was completed, in line with the Central YMCA's policies.

#### Remedial steps taken by the Central YMCA

1.13 The Commissioner has also considered and welcomes the remedial steps taken by the Central YMCA in light of this incident. In particular, the Central YMCA notified all affected individuals of the incident, taking accountability the error and informing data subjects of the steps being taken, including reporting the incident to the ICO and conducting an internal review. The incident was reported to the data protection officer then escalated efficiently, and learnings following the incident were shared across the organisation.

1.14 The Central YMCA conducted an audit of how external communications were being undertaken across the organisation and issued a new External Communications Procedure that provides appropriate guidance to employees on sending emails securely. The

Central YMCA also reviewed and updated its data protection training programme.

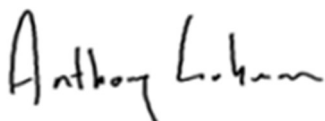
Decision to issue a reprimand

1.15 Taking into account all the circumstances of this case, including the remedial steps, the Commissioner has decided to issue a reprimand to the Central YMCA in relation to the infringements of Article 5(1)(f) and Article 32(1) and (2) of the UK GDPR set out above.

1.16 The Central YMCA has had an opportunity to make representations to the Commissioner in response to the Notice of Intent regarding this reprimand. Instead of making representations the Central YMCA has decided to accept the Notice of Intent and the Commissioner's findings.

1.17 The ICO considered notifying the Central YMCA of its intention to impose an administrative penalty in the amount of £300,000. 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 and issues this reprimand to the Central YMCA.

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