Information Commissioner's Office

DATA PROTECTION ACT 2018 (PART 6, SECTION 155)

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

TO: HIV Scotland

OF: 18 York Place, HIV Scotland, Edinburgh EH1 3EP

1. HIV Scotland is charity registered in Scotland (number SC033951) and a company limited by guarantee (number SC242242).

2. The Information Commissioner ("the Commissioner") has decided to issue HIV Scotland with a Penalty Notice under section 155 of the Data Protection Act 2018 ("the DPA"). This penalty notice imposes an administrative fine on HIV Scotland, in accordance with the Commissioner's powers under Article 83 of the General Data Protection Regulation 2016 ("the GDPR"). The amount of the monetary penalty is £10,000.

3. This penalty has been issued because of contraventions by HIV Scotland of Articles 5(1)(f) and 32(1) and (2) of the GDPR in that, during the period of 25 May 2018 to 24 February 2020, HIV Scotland failed to implement an appropriate level of organisational and technical security to its internal email systems. This failure resulted in an email being sent on 3 February 2020 without the appropriate security to 105 recipients, disclosing the personal data of 65 of the recipients. In particular, the email contained personal data and disclosed information from which special category data could be reasonably inferred.

4. In the interests of clarity, 25 May 2018 is the date when GDPR came into effect, and 25 February 2020 is the date on which HIV Scotland took its final steps to implement MailChimp as its sole email client for any mail-out across the organisation, thereby mitigating the risk which led to the initial data breach.

5. 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.

Legal framework for this Notice of Intent

Obligations of the controller

6. HIV Scotland is a controller for the purposes of the GDPR and the DPA, because it determines the purposes and means of processing of personal data (GDPR Article 4(7)).

7. 'Personal data' is defined by Article 4(1) of the 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.*

8. 'Processing' is defined by Article 4(2) of the 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*

9. Article 9 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 'data concerning health or data concerning a natural person's sex life or sexual orientation'.

10. Controllers are subject to various obligations in relation to the processing of personal data, as set out in the 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 GDPR.

11. 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*

12. Article 32 ("**Security of processing**") provides, in material part:

> *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

13. The Commissioner is the supervisory authority for the UK under the GDPR.

14. By Article 57(1) of the GDPR, it is the Commissioner's task to monitor and enforce the application of the GDPR.

15. By Article 58(2)(d) of the GDPR the Commissioner has the power to notify controllers of alleged infringements of GDPR. By Article 58(2)(i) she 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.

16. 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.

17. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner. Section 155 of the DPA ("**Penalty Notices**") provides that:

(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 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 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 GDPR or section 64 or 65 of this Act (obligations of controllers and processors) […]

Factual background to the incident

19. HIV Scotland is a charity which provides support for individuals living with HIV, individuals who may be at risk of HIV, and individuals who support those groups.

20. HIV Scotland's Community Advisory Network ("CAN") brings together patient advocates from across Scotland to represent the full diversity of people living with HIV. Individuals sign up to be part of this network to help support and inform the work of HIV Scotland. Semi-regular email updates are sent to the group, usually surrounding one of their quarterly meetings.

21. Having identified its online mailing/database programme as a key organisational priority in April 2019, in June 2019 HIV Scotland made a decision to procure a MailChimp account. The procurement took place in July 2019. Over the following months a number of lists held by HIV Scotland were migrated to MailChimp to provide the necessary functionality for bulk messages to be sent in a more secure manner. However, by the time of the incident, the CAN list was not one of those which had been migrated.

22. On 3 February 2020, [redacted] HIV Scotland sent an email using Microsoft Outlook, containing an agenda for an event taking place on 8 February 2020, to 105 individual members of HIV Scotland's CAN. The agenda provided details of the meeting's key discussion points, and details of the meeting's location. Instead of using the Blind Carbon Copy ("BCC") feature, the [redacted] used the Carbon Copy ("CC") feature, showing the email addresses of all intended recipients to all that received the email.

23. 65 of 105 email addresses visible to the other recipients as part of this communication clearly identified individuals by their name. The breach was identified immediately, [redacted] It has not been possible for HIV Scotland to determine how successful the recall was.

24. It is noted that two recipients responded to HIV Scotland to highlight the incident.

25. HIV Scotland contacted the ICO Helpline about the incident and completed and submitted a breach report on the same day as the incident. The incident was attributed to human error, with HIV Scotland accepting that, in terms of the personal data disclosed, "*[a]ssumption could be made about individuals HIV status or risk*".

26. Upon becoming aware of the error, HIV Scotland's chief executive emailed all recipients to apologise. HIV Scotland also issued a statement on its website, contacted the individuals involved to apologise, and to ask that the email is deleted. It also offered personal support in the event of any distress caused. HIV Scotland has advised that 12 individuals contacted it to thank it for the apology.

27. [redacted]

28. It is understood that MailChimp is now fully implemented and operational so the risk of a repeat incident is significantly reduced and very unlikely. In February 2020 HIV Scotland confirmed to the Commissioner that it has "*now completed the migration to MailChimp to ensure that the error of failing to BCC a group email can no longer occur.*" [redacted]

29. As a result of the breach, HIV Scotland decided to fully audit all of its security and data management procedures and a full search of its SharePoint Server was completed to ensure no personal information was stored separately from its secure mailing lists.

30. The Commissioner has considered whether these facts constitute a contravention of the data protection legislation.

The Contraventions of Article 5(1)(f), 32(1) and (2) of the GDPR

31. For the reasons set out below, the Commissioner takes the view from her investigation that this breach occurred primarily as a result of serious deficiencies in HIV Scotland's technical and organisational measures.

32. It is accepted that HIV Scotland did have some policies and associated measures, whether in place or in progress, at the time of the breach, and the Commissioner has considered these below:

a) HIV Scotland advised that all employees would be asked to read and refer to the HIV Scotland's Privacy Policy as well as highlight it to those who contact them when relevant.

b) HIV Scotland confirmed that all staff have access to an online training hub called 'BOLT Spark' and are required to complete 11 training modules within the first three months of their employment, including GDPR (called "*EU GDPR Awareness for All*") which contains an assessed module on data protection and specifically GDPR.

c) HIV Scotland stated that the [redacted] was aware of the privacy policy and expectations to meet GDPR requirements, including the use of BCC for group emails.

d) HIV Scotland were at the time of the breach in the process of migrating its databases/lists to MailChimp in order to introduce the ability to securely email group contacts on all mailing lists held by them.

33. Whilst it is accepted that HIV Scotland had taken some steps as detailed above, the Commissioner finds that they were not sufficient. The Commissioner's findings are detailed below:

a) HIV Scotland did not have a specific Policy on the secure handling of personal data within the organisation. Rather, the Policy staff relied on related to HIV Scotland's own Privacy Policy, and was the public facing statement covering points such as Cookie use, and data subject access rights; it was not an appropriate Data Protection Policy which focused on staff handling of personal data. The Privacy Policy referenced by HIV Scotland provided no guidance to staff on the handling of personal data itself, for example, what they must do

to ensure that it is kept secure. This is something which the Commissioner would expect from an organisation handling personal data, and would expect it to maintain policies regarding, amongst other things, confidentiality.

b) The [redacted] used by HIV Scotland includes an entry for day one as "*Explanation of data processing, GDPR & email use inc. BBC for group emails*" *(sic)* which appears to suggest that the use of BCC for group emails was deemed an acceptable method of group-email contact.

c) HIV Scotland stated in its initial breach notification, that the [redacted]

HIV Scotland confirmed that employees are expected to complete the "*EU GDPR Awareness for All*" on an annual basis. The Commissioner considers it a weakness and a risk that the data protection course is expected to be completed [redacted] when it should have been much sooner and certainly before an employee handled personal data. Whilst there is no fixed requirement within the DPA or the GDPR as to the type of data protection training an employee should undertake, or when it should be provided, as part of a controller's organisational measures to safeguard personal data the Commissioner would expect an organisation to train employees handling personal data, and in particular data which is special category in nature or by inference before an individual is given access to such data. The Commissioner's current guidance on this (as contained in the

'Accountability Framework' package[1]) recommends that staff receive induction training prior to accessing personal data and within one month of their start date.

d) Regarding the implementation of Mailchimp, the Commissioner notes that when asked for its reasons for procuring Mailchimp, HIV Scotland advised that "*when I [*the HIV Scotland representative*] took over as Chief Executive, the system for storing data was poor in the organisation. It involved a variety of different excel spreadsheets that individual staff controlled. This meant that if someone asked to be removed from a mailing list; the process was difficult and hard to confirm every entry had been deleted. When we hired our Communications Lead, we highlighted an online mailing/database programme as a key priority in April 2019." (sic)*.

HIV Scotland stated further during the Commissioner's investigation that "*[d]ue to the impending event, we had not yet moved the Advisory Network mailing list over to MailChimp to ensure everyone was still receiving the emails."* The "impending event" referred to is the CAN event of 8 February 2020, to which the email agenda that was sent on 3 February 2020 without the use of BCC pertains. HIV Scotland further confirmed that they had procured MailChimp and other groups had been transferred onto it, but they held off doing that for this particular CAN group because of the immediacy of the event that formed the content of the email of 3 February 2020. They were concerned that if they had used MailChimp for communication in relation to the impending event, that the emails may have caused disruption by ending up in the junk folder or appearing to have been sent by someone else. It is clear from HIV Scotland's reasons for procuring Mailchimp that it had identified the

[1] https://ico.org.uk/for-organisations/accountability-framework/training-and-awareness/induction-and-refresher-training/

need for improvements to online mailings as early as ten months prior to the breach.

The Commissioner understands that Mailchimp was in fact procured in July 2019 but was not adequately implemented by the time of the breach on 3 February 2020.

Mailchimp provided the necessary functionality for bulk messages to be sent in a more secure manner. The Commissioner is of the view that if it had been appropriately implemented when communicating with users and supporters of HIV Scotland's services via email, it would have prevented the disclosure of those users' email addresses. In short, it would have prevented both the occurrence and consequence of the breach.

The Commissioner's investigation into this matter has determined that despite a clear recognition of the risks of the use of BCC, insufficient steps were taken quickly enough to prevent the disclosure of service users' emails. This is despite a solution having already being procured and in use in regard to other areas of HIV Scotland's estate. This represents a serious and negligent failure to take appropriate organisational and technical steps to reduce the possibility of an incident occurring. If the use of Mailchimp had been adequately risk assessed, scoped and prioritised, the Commissioner takes the view that it is highly likely that this incident would not have happened.

34. The Commissioner considers that the data concerned in this case comprises of email addresses. An email address which clearly relates to an identified or identifiable living individual is considered to be personal data.

35. However, regarding the content of any email, this will not automatically be personal data unless it includes information which reveals something about that individual or has an impact on them.

36. In this case, it is considered that the content of the email, specifically the agenda, combined with the identity of the organisation sending the email, does reveal information about the recipients. Namely, the receipts are identified as HIV Scotland CAN members, to the extent that they have been invited to a CAN event hosted by the organisation. Consequently, and to the extent to which 65 individuals can be identified from the email distribution list, special category data can be inferred to a reasonable degree in so far as the disclosure of the email addresses connects those individuals with an organisation that provides HIV support services.

37. The Commissioner takes the view that even if the email addresses and content of the email itself can be deemed not to constitute special category data, it is clear that there are particular sensitivities around the nature of the personal data being processed in this situation that HIV Scotland should have considered in line with the Commissioner's guidance on Special Category Data[2].

38. The Commissioner considers further that HIV Scotland has previously demonstrated an increased awareness of the risks of such conduct, given that on 17 June 2019 it had commented critically on its website in relation to a similar issue involving a Health Board.

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7

39. The Commissioner takes the view that by the time the HIV Scotland breach occurred almost eight months later, and having commented on the error experienced by another controller, HIV Scotland were certainly aware of such a risk and should have ensured they had adequate measures in place to prevent such an incident within its own organisation.

40. HIV Scotland has confirmed that it received one formal complaint regarding the incident but did not believe the points raised in the complaint required any further action. HIV Scotland responded to the complainant with its view at the time, although the Commissioner considers that the complaint clearly identifies distress being experienced by the complainant as a result of the breach.

41. Specifically, with regard to the principle of integrity and confidentiality under Article (5)(1)(f) of the GDPR, the Commissioner considers that HIV Scotland failed to send a separate email to each intended recipient, and instead utilised the bulk email facility.

42. The Commissioner further finds that, notwithstanding its failure to migrate the CAN list to the more secure MailChimp platform despite it being available, HIV Scotland failed to use the BCC function of Microsoft Outlook.

43. [redacted] had completed the '*Explanation of data processing, GDPR & email use inc BBC for group emails' (sic)* awareness training [redacted]

44. In regard to the requirement under Articles 32(1) and (2) of the GDPR to implement a level of security appropriate to the risk when processing data, the Commissioner considers that HIV Scotland failed to implement a level of security appropriate to the risk in this instance. HIV Scotland had actively recognised the need for greater outbound mailing security a number of months prior to the breach, and had in fact procured a MailChimp account which, if implemented, would have mitigated the risk of a breach. However, it failed to implement this level of security in relation to the CAN list which, had it done so, would have significantly reduced the likelihood of the breach occurring.

45. The Commissioner finds that HIV Scotland should have taken particular account of the risks associated with processing the personal data in this instance when assessing the appropriate level of security. Given the nature of the CAN list, together with the significant delay between procurement of MailChimp in July 2019 and its eventual implementation which took place shortly after the breach in February 2020, it is clear that HIV Scotland failed to do this.

Notice of Intent

46. On 22 July 2021, in accordance with s.155(5) and paragraphs 2 and 3 of Schedule 16 DPA, the Commissioner issued HIV Scotland with a Notice of Intent to impose a penalty under s.155 DPA. The Notice of Intent described the circumstances and the nature of the personal data breach in question, explained the Commissioner's reasons for a proposed penalty, and invited written representations from HIV Scotland.

47. On 20 August 2021, HIV Scotland provided written representations in respect of the Notice, together with supporting documentation in relation to its finances.

48. On 30 September 2021 the Commissioner held a 'representations meeting' to thoroughly consider the representations provided by HIV Scotland. At that meeting it was determined that a monetary penalty remained appropriate in all of the circumstances.

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

49. The Commissioner has considered the factors set out in Article 83(2) of the GDPR in deciding whether to issue a penalty. For the reasons given below, she is satisfied that (i) the contraventions are sufficiently serious to justify issuing a penalty in addition to exercising her 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

50. On 3 February 2020 [redacted] sent an email using Microsoft Outlook to 105 individual members of HIV Scotland's CAN. The email contained an agenda for a forthcoming meeting. Instead of using the BCC feature, [redacted] used the CC feature, showing the email addresses to all that received the email. This was a one-off incident.

51. 65 individuals could potentially be identified as their names were included in the email address. The other email addresses did not have identifiable information in the email address but could be used to identify individuals in combination with other information e.g. the email address could be used to search online to discover other details about

the individual. Whilst the data comprises email addresses which in themselves are not considered special category data, it could be inferred that the individuals they belong to are HIV positive or supporting someone who is.

52. The Commissioner considers that it is at least possible that there may be an element of distress associated with this breach. There has been one formal complaint received by HIV Scotland, with the complainant stating that their HIV status had been disclosed to strangers and their choice to tell friends or family had been taken away.

(b) the intentional or negligent character of the infringement

53. The Commissioner considers that there is no evidence of there being an intentional aspect to this infringement, however the Commissioner considers that the breach was negligent since the risks of using Outlook for sensitive communications were known by HIV Scotland either by reference to previous ICO enforcement action, or by HIV Scotland's knowledge of a very similar recent incident involving another controller. Furthermore, online mailing was a key priority area identified by HIV Scotland in April 2019, some ten months before the breach occurred. MailChimp was procured in July 2019 and yet the CAN group was still not migrated to MailChimp by 3 February 2020. There was also a degree of negligence in that HIV Scotland's policies and procedures, and also the [redacted] was not sufficient at the time of the incident.

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

54. All affected recipients were emailed by HIV Scotland, and a statement was put on its website very shortly after the incident occurring. HIV Scotland also asked all recipients to delete the email. In addition, the matter was addressed at the CAN meeting on 8 February 2020 when HIV Scotland outlined the action it had taken and offered the chance for queries or concerns. The sole complaint has been dealt with.

(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

55. HIV Scotland should have been aware of previous, very similar incidents that the ICO has fined and publicised. They were certainly aware of a case involving a UK controller that occurred in June 2019 and identified the need for a different system. MailChimp was procured but 7 months had passed and the CAN group had not yet been migrated to MailChimp at the time of the incident. HIV Scotland should have adopted a risk-based approach and should have identified the CAN list as one of the more urgent groups, noting the potential for the inference of special category data; it is for this reason that the Commissioner is of the view that it should have prioritised its migration. Whilst HIV Scotland's [redacted] materials suggested that 'BCC' was sufficient as a means of engaging in group emails, it should have identified that this was a risk and at the very least put other measures in place such as not sending group emails out and sending such emails individually until MailChimp was fully implemented.

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

56. The Commissioner is unaware of any previous data protection infringements by HIV Scotland.

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

57. HIV Scotland were fully cooperative with the Commissioner's investigation.

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

58. Whilst the disclosed data comprises email addresses which in themselves are not considered special category data, the Commissioner is of the view that it can be reasonably inferred that the individuals whose email address were impacted included individuals who are HIV positive or at risk of contracting the virus.

(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

59. HIV Scotland notified the Commissioner about the breach on 3 February 2020. HIV Scotland contacted the Commissioner's Helpline about the incident and completed the necessary 'breach report' within 2 hours of the incident occurring.

(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;

60. Not applicable.

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

61. 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.

62. The Commissioner has considered the following **aggravating factor** in this case:

- The Commissioner has previously taken action against organisations for similar breaches. As such, the Commissioner takes the view that the risks of these kind of disclosures and the consequences for the potential harm that might be caused to data subjects was a matter that had been reported on both in mainstream and trade (privacy professional) media.

63. The Commissioner has considered the following **mitigating factors** in this case:

- [redacted] are asked to read and refer to HIV Scotland's privacy policy – whilst this does not provide sufficient guidance or information generally about what [redacted] are required to do, it demonstrates that data protection considerations are not entirely absent from HIV Scotland's induction process.

- MailChimp had been procured but at the time of the breach the CAN group had not been migrated. The plan was that the group would be told about this at the meeting on 8 February 2020 so that they would be aware and to avoid emails going to 'Spam' or it not being clear who they were from. Full migration to MailChimp is now completed. Whilst the failure to implement this solution quickly is a material fact to the seriousness of the

infringements, its procurement demonstrates that consideration of the improvements that could be made, specifically the security of email communications, was not entirely absent.

- The organisation has a training portal for [redacted] with mandatory GDPR training refreshed every year.

- HIV Scotland took steps to remedy the incident by asking all recipients to delete the email on the same day that it was sent, and also added a message to its website.

Summary and decided penalty

64. For the reasons set out above, the Commissioner has decided to impose a financial penalty on HIV Scotland. The Commissioner has taken into account the size of HIV Scotland, publicly available information regarding its finances, and the representations made by HIV Scotland as to its financial position. She is mindful that the penalty must be effective, proportionate and dissuasive.

65. Taking into account all of the factors set out above, the Commissioner has decided to impose a penalty on HIV Scotland of **£10,000** (**ten thousand pounds**).

Payment of the penalty

66. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by **16 November 2021** at the latest. The 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.

67. 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

68. Any notice of appeal should be received by the Tribunal within 28 days of the date of this penalty notice.

69. 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.

70. 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.

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

Dated the 18th day of October 2021

Stephen Eckersley
Director of Investigations
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

DATA PROTECTION ACT 2018

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:

   General Regulatory Chamber
   HM Courts & Tribunals Service
   PO Box 9300
   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))