DATA PROTECTION ACT 2018

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Cabinet Office

Of: 70 Whitehall, London, SW1A 2AS

1. The Information Commissioner ("the Commissioner") has decided to issue the Cabinet Office with a penalty notice pursuant to section 155 of the Data Protection Act 2018 ("DPA"). This penalty notice imposes an administrative fine on the Cabinet Office, in accordance with the Commissioner's powers under Article 83 of the GDPR. The amount of the penalty is £500,000 (five hundred thousand pounds).

2. The penalty is being issued because of contraventions by the Cabinet Office of Articles 5(1)(f) and 32(1) of the GDPR in that, on 27-28 December 2019, the Cabinet Office in error published on GOV.UK a CSV file which included full correspondence (postal) addresses of [redacted] data subjects (all of whom were 2020 New Year Honours recipients), resulting in a disclosure of personal data. This was a breach of Article 5(1)(f) of the GDPR as the Cabinet Office did not process personal data in a manner that ensured appropriate security of the personal data. Further, at the time of and in the run up to the aforementioned breach, the Cabinet Office did not have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing of data for the purpose of the 2020 New Year Honours List in breach of Article 32(1) of the GDPR.

3. This penalty notice explains the Commissioner's reasons for imposing such a penalty, and for the amount of the penalty. Prior to issuing this penalty notice, the Commissioner carefully considered the Cabinet Office's Response to Notice of Intent dated 16 September 2021.

Legal Framework

4. The Cabinet Office is a data controller for the purposes of the GDPR and DPA 2018 because it determines the purposes and means of the processing of the personal data associated with this incident (Article 4(7) of the GDPR).

5. "Personal data" is defined by Article 4(1) of the GDPR to mean:

> *"any 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"*

6. "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"*

7. Data controllers are subject to various obligations in relation to the processing of personal data as set out in the GDPR and DPA 2018. They are obliged by Article 5(2) of the GDPR to adhere to the data processing principle set out in Article 5(1).

8. Article 5(1)(f) of the GDPR provides 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 ('integrity and confidentiality')".*

9. Article 32 of the GDPR provides:

> *"(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."

10. The Commissioner is the supervisory authority for the United Kingdom as provided for by Article 51 of the GDPR.

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

12. By Article 58(1)(d) of the GDPR, the Commissioner has the power to notify controllers of alleged infringements of the GDPR. By Article 58(2)(i), the Commissioner 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 circumstance of each individual case.

13. 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.

14. Article 83(2) goes on to set out a number of factors to which the Commissioner should have regard when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case.

15. The DPA 2018 contains enforcement provisions in part 6 which are exercisable by the Commissioner. Section 155 DPA 2018 provides in relevant part:

> *"(1) If the Commissioner is satisfied that a person—*
> *(a) has failed or is failing as described in section 149(2), (3), (4) or (5), …*
> *the Commissioner may, by written 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 UK GDPR applies, the matters listed in Article 83(1) and (2) of the UK GDPR*
>
> *…"*

16. Section 149(2) DPA 2018 provides in relevant part:

> *"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)*
>
> *…"*

Background Facts

Overview

17. On Friday 27 December 2019 at 22:30 the Cabinet Office published the content page for the New Year 2020 Honours List on GOV.UK. This was completed via a scheduled automatic publication set up by the Cabinet Office Publishing Team.

18. The content page as published contained a link to a comma-separated values ("CSV") file version of the Honours list, which in error included the correspondence (postal) addresses of Honours recipients. This resulted in an unauthorised disclosure affecting [redacted] data subjects across the United Kingdom [redacted]

19. The Cabinet Office Press Office was alerted to the data breach by a member of the Government Communications Team who had *"identified the data breach by chance"*. After becoming aware of the breach, at 22:59 on 27 December 2019 the Cabinet Office Publishing Team republished the content page removing the link to the CSV file. However, as files uploaded onto GOV.UK are automatically cached on a content delivery network, the file continued to be accessible online to people who had the exact webpage URL.

20. The Cabinet Office contacted the Government Digital Service (GDS) at 23:34 for GDS to assist with removing the CSV file, as although the Cabinet Office can edit pages and remove links, they cannot remove documents from the GOV.UK website once they have been published. [redacted] the issue was escalated within GDS and support was obtained

from a developer. This resulted in the CSV file being permanently deleted at 00:51 on 28 December 2019.

21. Therefore, in total, the CSV file containing the postal address data was accessible from 22:30 on 27 December 2019 to 00:51 on 28 December 2019 - a period of two hours and 21 minutes. During that time the CSV file was accessed 3,872 times from 2,798 IP addresses.

22. Although the file was accessible via the cache until 00:51, the Cabinet Office Publishing Team republished the content page at 22:59 which removed the link to the file. The Cabinet Office's logs show most of the access to the file (72%) occurred in the initial period before the link was removed and access declined over time.

23. Affected data subjects were contacted within 48 hours of the data breach via email or telephone (if data subjects did not have an email address, the email had bounced back, or if there was an out-of-office message) where possible on 28 and 29 December 2019. Approximately 11 data subjects were not contactable via either telephone or email and needed a hard copy letter to be posted to them. Following this, a hard copy letter was posted to all affected data subjects on 30 December 2019.

24. The Cabinet Office submitted a Personal Data Breach Report to the ICO within 72 hours of becoming aware of the data breach in accordance with Article 33(1) of the GDPR.

Circumstances surrounding the data breach

25. The Honours and Appointments Secretariat ("HAS") in the Cabinet Office coordinates the Honours system and processes all public nominations.

26. A new IT system [redacted] was introduced within HAS in 2019. [redacted] was built between January and June 2019 and was in use from July 2019. The 2020 Honours round was the first to use the new [redacted] system.

27. The report [redacted] which generated the CSV file was incorrectly formulated to include postal address data which it should not have done and was not an element requested in the original build requirements. The Cabinet Office's Digital and Technology Team was responsible for building the system.

28. Although testing took place on the [redacted] report by the Cabinet Office's Digital and Technology Team and the HAS Operations Team, the postal address column went unnoticed during the testing process which the Cabinet Office has said they believe was due to the large number of fields in the spreadsheet and the focus on ensuring the list of successful Honours recipients was accurate.

29. A 'desk note' of instructions had been produced to articulate the process for running the [redacted] reports which produce the final Honours lists. These instructions were available to employees via Google Drive. However, these instructions reflected the [redacted] report as it should have been set up and did not include a check to ensure personal data that should not have been included therein was removed.

30. On 19 December 2019, the error with the [redacted] report incorrectly including postal address data was identified by the HAS Operations Team. However, due to short timescales between finalising amendments to the list and the deadline for giving the lists to the Press Office for publication *"the decision was taken to amend the output as opposed to the report build itself".*

31. On 23 December 2019 following certain changes to the Honours list, a second report was run to generate the CSV file for publication. This was completed by an employee not usually responsible for the process. This employee *"was aware that postal address information should not be in the report and altered it to hide the information".* Due to this, the CSV file incorrectly included postal address data which had been hidden but was still contained in the document as it had not been deleted. The Cabinet Office has subsequently stated *"we acknowledge that the information should have been deleted".* This version of the CSV file was sent to the Press Office on the same date.

32. On 24 December 2019 a [redacted] opened and reviewed the documents sent to the Press Office on 23 December 2019 and identified formatting errors which needed correcting. The [redacted] emailed the HAS Operations team on 24 December 2019 to highlight the formatting errors. The Cabinet Office said inclusion of the postal address data was not identified by the [redacted] as it was not visible. In relation to this event, the Cabinet Office said, *"In retrospect, this incident should have then automatically triggered a formal review point to check that the final version was correctly amended."*

33. On 24 December 2019 a third and final report was run [redacted] to make the corrections requested by the [redacted]. This report again generated a CSV file incorrectly including postal address data.

34. As the postal address data was hidden, the employee sending the document to the Press Office on 24 December 2019 thought the postal address data had been removed when *"in reality it was still there and became visible when the document was uploaded to gov.uk".* When asked if it was the same employee who hid the data as who sent the document to the Press Office, the Cabinet Office confirmed two people were involved in the process.

35. The Cabinet Office's internal investigation report said the email sent to the Press Office on 24 December 2019 "*was copied to the* [redacted] *and a small number of HAS members, but did not include the relevant Director or senior press office staff".* The Cabinet Office confirmed that the [redacted] copied into the email was the same person who identified the formatting errors with the version produced on 23 December 2019. However, the [redacted] was on annual leave on 24 December 2019 when the final version was sent to the Press Office.

36. The Press Office received the final version of the CSV file on 24 December 2019, which incorrectly included the postal address data. It is understood the covering email "*indicated that the previous issue had been resolved"*. The final CSV file was not opened by the Press Office before they completed a web publication form and sent this and the documents they had received to the Digital Team for publication on the same date, as they relied upon reassurance from the HAS in the covering email that the document was the final version. The Cabinet

Office stated that *"the press office and digital teams were not responsible for reviewing the data for sensitivities of this type".*

37. On 27 December 2019 the Press Office checked with the HAS that there had been no further changes and were told by the [redacted] that this was correct. Therefore they *"assumed that the document was still the final version to publish".*

38. On 27 December 2019, the work to prepare the publication was completed by the Digital Team. At this point the Digital Team checked with the Press Office that there had been no changes to the documents. Checks for formatting, accessibility standards and correct functionality were completed by the Digital Team as per the standard process. However, these did not include any assessment of the substance, *"as the team is not best placed to make any judgements"* on the content and *"it is clear that the documents need to be final signed-off versions".* The documents were subsequently included in the content page for automatic publication.

39. The Cabinet Office has stated that *"it has always been standard practice for the* [HAS] *Team to undertake a final review of the list documents before publication to ensure, for example, that there is no sensitive data present and that the information is presented in the correct format. This review is not intended to require or result in extensive amendments, as that would indicate that the underlying data had been incorrectly entered in the database or that the report had been set up wrongly".* However, the Cabinet Office confirmed there was no specific or written process in place in the HAS to sign-off or approve documents containing personal data prior to being sent for release to ensure the content was suitable for publication.

40. The Cabinet Office's internal investigation report included three recommendations for improvement following the incident, demonstrating certain measures were not present at the time the data breach occurred:

a. Recommendation 1: That the Honours IT system is updated and re-tested to ensure that a publication-ready document is produced when the report is run, which does not include address or other sensitive data. The Desk Instructions should be amended to ensure the report is always checked so that it only ever includes data that can be published.

b. Recommendation 2: Ensure clear line of accountability for sign off for documents that will be published and that there are clear instructions in the email, which give sufficient detail so others can check.

c. Recommendation 3: Press Office and Digital Communications ensure that the process for removing documents published in error is clearly understood, including for out of hours.

41. An independent review led by Adrian Joseph and commissioned by the Cabinet Office reviewed wider data handling processes/practices within the Cabinet Office. That review includes the following observations:

"Breaches, such as the one that impacted New Year's Honours recipients in December 2019, are too easily assigned to human error where a greater consistency of process, controls and culture across Cabinet Office could have reduced the risk systemically. There is a significant risk that further and more impactful breaches

will occur as the amount of personal data being handled by the Department increases.

…

The Cabinet Office identified two main factors that had contributed to the breach: the introduction of a new IT software package, which had included an additional field with individuals' addresses; and a lack of clarity about sign-off processes for the final versions of the documents that went online, and in the context of the new IT system."

42. The review also highlighted the following concerns relevant to the incident:

a. Whilst different documents exist on the Cabinet Office's intranet page regarding best practice on data handling, these documents are not regularly updated or promoted throughout the Department; *"The GDPR Hub, for example, has not been updated since May 2019"*.
b. There appear to be issues with access restrictions which are *"often imposed too late and there are examples of personal data being accessible to whole teams"*.
c. Cabinet Office structures regularly change with new business units often being stood up to deliver on urgent political priorities. *"The pace required to deliver on these priorities was cited by some business units and stakeholders as potentially compromising the disciplines of good personal data handling"*.
d. Some teams have built additional checks into their processes, including validating data being transferred between Government Departments, *"however, in some instances it would be possible to eliminate human error altogether by fixing failings in IT systems. For example, in one software system it*

is possible to accidentally send personal information about one individual to another, unconnected, individual whose details are also held in the same system".

e. *"Interviewees raised a number of concerns around the procurement of new software to run their data handling processes. Some said that financial considerations meant that off-the-shelf solutions were chosen to run processes that, given their complexity, warranted bespoke solutions"*.

f. *"Another concern raised by a number of teams was that software had not undergone sufficiently robust or extensive testing in advance of being rolled out. The reasons cited included lack of both staff and money, lack of expertise within the commissioning teams, and projects being rolled out too quickly in order to meet Ministerial commitments. In all instances considered by the Review these risks had been signed off by senior managers or Ministers"*.

g. *"…training is not monitored across the organisation. One team interviewed for the Review had set up their own training log, but most did not actively monitor which members of their teams had completed the training"*.

Apology

43. On 7 January 2020, the Minister for the Cabinet Office made a statement to Parliament by which the Cabinet Office gave a public apology in relation to the incident.

Notice of Intent

44. On 4 August 2021, in accordance with section 155(5) and paragraphs 2 and 3 of Schedule 16 DPA 2018, the Commissioner issued the Cabinet

Office with a Notice of Intent to impose a penalty under section 155 DPA 2018. The Notice of Intent described the circumstances and the nature of the personal data in question, explained the Commissioner's reasons for the proposed penalty of £600,000, including what she regarded as the aggravating and mitigating factors, and invited written representations from the Cabinet Office.

45. On 16 September 2021, the Cabinet Office provided written representations in response to Notice of Intent. The key representations made by the Cabinet Office were:

a. the level of the fine is disproportionate to the scale of the breach (particularly taking into account that of the addresses revealed the majority were already readily accessible in the public domain);

b. the proposed penalty does not take into account the extensive immediate and long-term action taken by the Cabinet Office to mitigate the consequences of the breach and was not determined in accordance with the statutory guidance reflected in the Commissioner's Regulatory Action Policy;

c. the proposed penalty does not adequately reflect the statement made to Parliament by the Minister for the Cabinet Office on 7 January 2020 and the apology contained within that statement and this statement does not appear to have been taken into account adequately when the Notice of Intent was formulated; and

d. The breaches do not warrant an administrative penalty and that another sanction such as that set out Article 58(2)(b) GDPR would be more appropriate.

46. The Cabinet Office's representations have been considered in full. Having taken these representations and all other factors into account, the Commissioner has decided to issue a monetary penalty in the sum of £500,000.

Breaches of GDPR

Contravention of Article 5(1)(f) of the GDPR

47. Article 5(1)(f) of the GDPR has been contravened as the Cabinet Office, the controller, published the CSV file on GOV.UK which included full correspondence (postal) addresses of [redacted] data subjects in error, resulting in a disclosure of personal data.

48. By Article 5(2) it is the controller who is responsible for and must be able to demonstrate compliance with Article 5(1).

Contravention of Article 32 of the GDPR

49. Article 32(1) of the GDPR has been contravened as the Cabinet Office, the controller, did not have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing of data for the purpose of the 2020 New Year Honours List.

Exemptions

50. Paragraph 15 (1) of Part 2 of Schedule 2 to the DPA 2018 provides:

"The listed GDPR provisions do not apply to personal data processed for the purposes of the conferring by the Crown of any honour or dignity."

51. Paragraph 6 of Part 2 of Schedule 2 to the DPA 2018 provides (emphasis added):

"In this Part of this Schedule, "the listed GDPR provisions" means the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the GDPR)—

(a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);
(b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);
(c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);
(d) Article 16 (right to rectification);
(e) Article 17(1) and (2) (right to erasure);
(f) Article 18(1) (restriction of processing);
(g) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);
(h) Article 20(1) and (2) (right to data portability);
(i) Article 21(1) (objections to processing);
(j) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (a) to (i).€

52. The contravention of Article 5(1)(f) of the GDPR in the present case arises from a data security incident not from the rights and obligations at paragraph 6(a)-(i) of Part 2 of Schedule 2 to the DPA 2018 – the exemption therefore does not apply.

The Regulatory Action Policy

53. When deciding to impose a monetary penalty and when setting the amount of that penalty, the Commissioner had regard to and acted in accordance with the Regulatory Action Policy.

54. In deciding to impose a monetary penalty, the Commissioner had regard to all of the factors set out on page 24 of the Regulatory Action Policy and assessed this case objectively on its own merits. In all the circumstances, a monetary penalty was considered appropriate given:

    a. the number of individuals affected;
    b. there was a degree of damage or harm (which may include distress and/or embarrassment); and
    c. there was a failure to apply reasonable measures to mitigate any breach (or the possibility of it).

55. In setting the amount of the penalty, the Commissioner applied the five step approach set out in the Regulatory Action policy:

    a. At step 1, the Commissioner determined that there were no discernible financial gains identified or losses avoided in relation to the incident.
    b. At step 2, the Commissioner had regard to the scale and severity of the breach by taking into account the considerations identified in s155(2)-(4) DPA 2018.
    c. At step 3, the Commissioner determined that there were no additional aggravating factors.

d. At step 4, the Commissioner determined that in view of the factors set out below, an amount should be added to the penalty otherwise payable in order to act as a deterrent.
e. At step 5, the Commissioner determined that there were no other factors (including ability to pay) on which to reduce the amount of the monetary penalty.

Article 83(2) GDPR

56. The Commissioner has considered the factors set out in Article 83(2) GDPR in deciding whether to impose a penalty and when deciding on the amount of the penalty as follows:

Nature, gravity and duration of the infringement

57. The data breach was a security incident whereby the confidentiality of personal data (postal addresses) was compromised by inclusion in the CSV file that was published in the public domain. The data breach was caused by or contributed to by the absence of appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing of the data in breach of Article 32(1).

58. The CSV file which contained the postal address data was live and publicly accessible in the public domain via GOV.UK for two hours and 21 minutes, - a relatively short duration. However, during the period in which the CSV file was accessible, where it could be either viewed in a web browser or downloaded, it was accessed 3,872 times from 2,798 unique IP addresses. Further, the Cabinet Office was well aware that the New Year's Honours list is a high-profile event which attracts considerable interest such that publication of this data set would place

the associated data in the public domain in a high demand arena, with accesses likely to take place quickly and on a relatively large scale.

59. Although the data disclosed was basic personal identifiers and, in error, location data (i.e. postal addresses) as opposed to more sensitive data such as special category data or criminal conviction data, the personal data disclosed related to [redacted] data subjects across the United Kingdom who are from a broad range of professions and include various high profile people. The personal data was published in the public domain and therefore accessible to anyone, as opposed to for example, being disclosed to other individuals who also had a high profile and therefore who would likely hold a shared interest in keeping the data secure.

60. The Cabinet Office confirmed that 207 data subjects out of a total of [redacted] affected had postal addresses that were not obviously in the public domain prior to the breach.

[redacted]

[redacted]

64. The Cabinet Office has stated that it has been informed by police[redacted] that there is no information to suggest an increased risk in relation to any persons as a result of the data breach.

65. There is, however, evidence that the data breach has caused distress to some of the affected data subjects. The ICO has received three complaints from affected data subjects raising personal safety concerns resulting from the breach. The Cabinet Office has also been contacted by 30 affected data subjects with 27 of those contacts relating to concerns about the possible impact on the individual's personal safety, largely as a result of pre-existing considerations.

66. The Cabinet Office also acknowledged in its initial breach report that the data breach gave rise to a possible increase in vulnerability to identity fraud, caused by the combination of names, postal addresses and, in a number of instances, the type of work they undertake being published.

67. The Cabinet Office further stated that *"To our knowledge, there has been a single instance, on 29 December, of a badly-redacted screenshot of the data being posted on Twitter. We asked Twitter to remove the tweet as a violation of their terms of service and this was carried out the same day"* and *"there is no evidence that the personal data involved in this incident has been inappropriately disseminated more widely, or indeed at all"*

68. In all the circumstances, the data breach was serious and could easily have been avoided. Further, the Cabinet Office had not implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The gravity of the failure was, then, very high.

Intentional or negligent

69. The infringements were negligent.

70. The data breach had the potential to occur due to a build error with the newly introduced IT system [redacted] within the HAS. Specifically, the report [redacted] which generated the CSV file was incorrectly formulated to include postal addresses in error. The original build requirements did not include a postal address field. The erroneous inclusion of the postal address data was not identified when the report was tested by Cabinet Office staff.

71. However, the error with the report functionality including the postal address data was identified by the HAS Operations Team on 19 December 2019. This date is before the data breach occurred and presented the Cabinet Office with the opportunity to implement

measures to sufficiently mitigate the risk and protect the data. The Cabinet Office did not do so.

72. Upon identification of the error with the report functionality *"the decision was taken to amend the output as opposed to the report build itself".* This was because of the short timescales between finalising amendments to the list and the deadline for giving the lists to the Press Office. Due to this decision, any outputs generated from the report would therefore continue to include the postal address data in error which would have left the data open to the risk of inadvertent publication. This is demonstrated by the data breach later taking place.

73. The ICO queried if all employees within the HAS were made aware of the requirement to remove the personal data (postal address data) before processing the generated reports once the error with the [redacted] report was identified by the HAS Operations Team. The Cabinet Office confirmed only 22 people have access to the [redacted] system. Information about the report functionality was relevant to only five members of the HAS Operations Team. These five employees were verbally advised of the requirement to remove the postal address data. However, employees were not issued any guidance on how to remove the data. The Cabinet Office said as [redacted] *"was a new system, and in effect a new process, the team were responsible for identifying solutions to the issues identified throughout the process"*

74. Employees relied on the desk note to produce the [redacted] reports which did not reflect the report as it was set up, and did not include a check to ensure personal data that should not have been included was removed.

75. Additionally, there was no specific or written sign-off process in place in the HAS before sending documents containing personal data for release to ensure the content was suitable for publication, even after formatting errors were identified in the second version of the CSV file when it was delivered via email to the Press Office. In relation to the formatting errors with the second version of the CSV file, the Cabinet Office said, *"In retrospect, this incident should have then automatically triggered a formal review point to check that the final version was correctly amended".*

76. The Cabinet Office had the opportunity on at least two occasions to implement measures to mitigate the risk and protect the data from a potential breach; firstly when the error with the report functionality including postal address data was identified by the HAS Operations Team on 19 December 2019, and secondly when the [redacted] identified formatting errors with the second version of the CSV file sent to the Press Office on 23 December 2019.

Action taken by the data controller to mitigate the damage suffered by data subjects

77. The Cabinet Office has undertaken a number of appropriate and effective remedial measures after becoming aware of the data breach as follows:

<u>To contain the incident</u>

a. Once the data breach was identified the Cabinet Office subsequently removed the link to the file on the content page and contacted GDS to remove the file from cache.

b. The Cabinet Office's logs show the majority of access to the file occurred in the initial period before the link was removed at 22:59 and access declined over time until the file was permanently deleted. This demonstrates that the immediate attempts to remove access to the data likely contributed to reducing the level of access after this point.

c. The file was accessible from 22:30 on 27 December 2019 to 00:51 on 28 December 2019 (two hours and 21 minutes) which is a short duration. It is however noted that the quick identification of the incident was due to a member of the Government Communications Team identifying the data breach by chance.

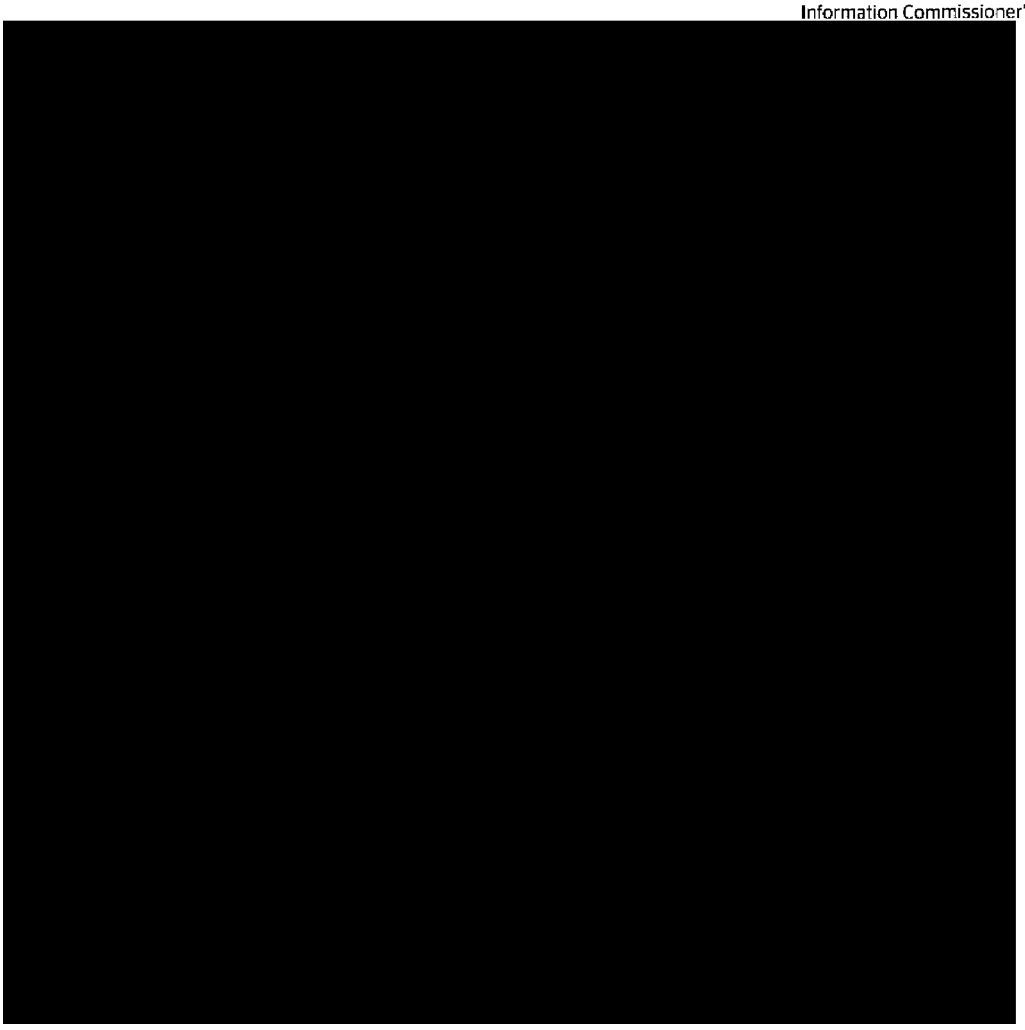
To inform data subjects

d. Affected data subjects were contacted within 48 hours of the data breach via email or telephone where possible on 28 and 29 December 2019. Approximately 11 data subjects were not contactable via either method and needed a hard copy letter posted to them. Following this, a hard copy letter was posted to all affected data subjects on 30 December 2019.

e. The HAS established a rota to answer recipient queries between 08:00-20:00 for the two weeks following the data breach.

To attempt to mitigate potential and actual damage caused to the data subjects

f. [redacted]



g. After being informed, actions were undertaken by the Police [redacted] to assess the risk to the affected data subjects in their area/region/locality. Where additional actions were required, this was taken forward by the relevant Police force [redacted] where appropriate. This included a reminder of security advice, data subjects being advised to contact 101 (excluding those who had contacted the HAS with specific issues) and placing additional protective flags at data subjects addresses etc. National Police Coordination Centre circulated a guidance document to all Police forces which could be circulated to individual Honours recipients wanting additional advice.

<u>To identify and prevent further dissemination of the personal data</u>

h. GDS used analytics to ascertain the extent of access to the data and were commissioned by the Cabinet Office to provide advice on further digital tracking and possible mitigation actions.

i. Cabinet Office staff monitored social media and arranged for a Twitter post which showed a screenshot of the data to be removed.

j. [redacted]

k. Internet monitoring was carried out by Police colleagues [redacted] for the first week and a half following the breach. Simultaneously, the Government continues to carry out its own monitoring which the ICO were told on 29 January 2020 will "remain for the foreseeable future". "This monitoring tracks instances of the data appearing online and seeks to identify obvious instances of the data being shared".

To reduce the likelihood of a similar event occurring in the future

l. GDS undertook a full incident review, including a review of checks on the publisher tool and incident handling. This review looked at how the escalation process works, publisher training, and technical changes that could have mitigated impact. This resulted in the caching time frame being reduced from 24 hours to 30 minutes for attached documents.

m. A number of actions have been undertaken in the Honours system specifically, this includes reviewing the overall security of the system and permission levels, an operational process review, the approvals process, reviewing the desk note of instructions, and creating a new report generated from their database which does not include postal information. Additionally, all employees in the HAS refreshed their Responsible for Information e-Learning after the breach.

n. Cabinet Office has confirmed "The report functionality in question has been amended to remove address data so that this does not arise in the future. Approvals processes for use from the (current) Birthday 2020 honours round will include a check to ensure that all documents for publication are checked for personal and sensitive data even when they should not contain it". The Cabinet Office have also provided a document with 16 action points where all except two have either had the work completed or they are currently in the process of doing so.

o. The Communications Team were taking action to ensure that anyone who has not recently undertaken training does so as soon as possible.

p. An independent review in the Cabinet Office led by Adrian Joseph OBE focusing on data handling policies, processes, practice and culture has been completed (dated March 2020) which includes recommendations for improvement.

Degree of responsibility

78. The data breach stems from a build error with a newly introduced IT system within the HAS. Specifically, the report [redacted] which generated the CSV file was incorrectly formulated to include postal address data in error. The original build requirements did not include a postal address field.

79. The Cabinet Office's Digital and Technology team were responsible for building the [redacted] system:

a. The [redacted] system was implemented under the agile project development process, with development being completed in periods called 'sprints' in which specific elements of the system were built, tested and approved. Required system functionality and any changes needed are articulated in project development software called JIRA which provides the audit trail for development.

b. In relation to JIRA, the Cabinet Office said *"User stories are defined and put into sprints for development. Each story outlines the requirements with clearly defined acceptance criteria. Stories are developed in a testing environment, then moved into the 'Testing' column where an internal functional test is carried out against the acceptance criteria. Once it has passed this test it moves into 'Product Owner Sign Off' where a member of the business unit checks the story. When the story has passed these checkpoints it moves to 'Done' and is deployed to the production environment. If necessary a training session is carried out with the business unit to walk through the story"*.

c. The period of the build between January and June 2019 was completed in two weeklong sprints and once the new IT system was in use from July 2019, the sprints became one month long.

d. The agile sprints included the delivery of system training to employees which included training on specific issues and was completed on numerous occasions throughout the year. Members of the Digital and Technology team were simultaneously co-located within the Honours Operations team for two days each week for several months to assist with issues, and all employees involved in this data breach knew how to use and had received training on the report functionality.

e. The [redacted] report functionality went through several tests and iterations before it reflected the correct candidates for the final Honours list. The report was tested by the both the Cabinet Office's Digital and Technology Team and the HAS Operations Team.

f. Not all staff in the HAS have access to the [redacted] system, which is a measure to control access to the material it contains. Only 22 employees have access.

80. Accordingly, there were measures in place regarding the initial building and testing of the [redacted] system/report. However, the error with the functionality of the [redacted] report including postal address data was not identified during this process.

81. There were also other measures in place within the Cabinet Office/HAS including:

a. The Cabinet Office had mandatory data protection training in place prior to the incident, which was primarily comprised of the Civil Service e-Learning course 'Responsible for Information'. This training had been completed by employees in the HAS. Each unit provides a six-monthly Information Assurance return which confirms that employees have completed training. The Cabinet Office said the training is part of induction to [the HAS] and a record is kept of completion.

b. There is a data hub on the Cabinet Office's intranet with guidance concerning all elements of the GDPR; information assurance (managing of information risks) including relating to the collection and sharing of personal data; the mandatory training; templates for data processing and privacy notices; and applied examples of best practice. The Cabinet Office said information is drawn to employees' attention via mechanisms such as a short cut to the hub on the intranet front page and staff communications. There are also additional, non-mandatory, learning courses about other elements of data handling on Civil Service Learning.

82. However:

a. When asked what percentage of Cabinet Office employees had completed the mandatory data protection training in the two years prior to the incident, the Cabinet Office confirmed there are seven modules in the "Responsible for Data" e-Learning which were completed between 3,517 and 4,070 times in the period encompassing the data breach. They were unable to provide a percentage but estimated take up of the training is

widespread *"but could vary between roughly half and most of the staff in the department at any given time".*

b. Employees in the Press Office and Digital Team, who were also involved in the process of the data being published, had not received data protection training in the last two years.

c. There was a 'desk note' of instructions which articulated the process for running the [redacted] reports which produce the final Honours lists available to employees via Google Drive. However, the desk note reflected the [redacted] report as it should have been set up. It did not include a check to ensure personal data that should not have been present was removed.

d. The Cabinet Office said the data hub does not cover redaction of documents to remove personal data and that *"Staff in the Secretariat were not explicitly trained on this point, in part because had the report been set up correctly, it should not have been necessary".* However, in mitigation to the above they said *"However, as part of their wider data training, they were aware that postal address information constituted personal data which should not be disclosed".*

This is particularly relevant to the data breach, as the employee involved believed that hiding the data in the CSV file involved in the data breach was a sufficient method to remove it.

e. There was no specific or written sign-off process in place in the HAS before sending documents containing personal data for release to ensure the content was suitable for publication, even after formatting errors were identified with the second version

of the CSV file when delivered via email to the Press Office. In relation to the identification of the formatting errors, the Cabinet Office said, *"In retrospect, this incident should have then automatically triggered a formal review point to check that the final version was correctly amended".*

f. As set out above, the error with the report functionality including the postal address data was identified by the HAS Operations team on 19 December 2019 before the data breach occurred, which presented the Cabinet Office with the opportunity to implement measures to sufficiently protect the data and mitigate the risk of it being handled incorrectly in error. The data breach later occurring demonstrates the risk of the postal address data being handled incorrectly was not sufficiently mitigated by appropriate technical and/or organisational measures. If the Cabinet Office had introduced further measures following the identification of the error with the [redacted] report, they could have reduced the likelihood of the postal address data being disclosed in error. Examples of such measures include:

    i. Amending the desk note to include robust and prescriptive instructions on the correct method to remove the postal address data in the CSV file generated which was not to be included in the list publication.

    ii. Implementing a sign-off procedure to check the postal address data had been removed correctly, in accordance with the instructions provided above, before delivering the final version to the Press Office for publication.

83. The nature of the publication of the Honours list is and was such that the document may need regular changes, possibly at the last minute. This, coupled with the fact that some of the data on the spreadsheet referred to vulnerable (to reflect the terminology adopted by the Cabinet Office) or high-profile individuals, meant that the security measures involved should, in order to demonstrate effective organisational and technical controls, have been more detailed and taken greater care to address the risks presented in the processing of the data set, including its eventual publication.

Any relevant previous infringements

84. No relevant previous infringements have been identified.

The degree of cooperation with the Commissioner

85. The Cabinet Office has been cooperative and responsive with the ICO's investigation. In particular:

a. The initial Personal Data Breach Report for the data breach was submitted within 72 hours of becoming aware, in line with Article 33 (1) of the GDPR.
b. Two conference calls took place between the ICO and the Cabinet Office early-on in the ICO's investigation.
c. The Cabinet Office have answered four rounds of written enquiries sent by the ICO albeit some of the responses were not as clear as they might have been.
d. The Cabinet Office have been open with the ICO regarding the failures/factors which contributed to the data breach.

The categories of personal data affected by the infringement

86. The data disclosed was location data (i.e. postal addresses). Some of the data affected was already in the public domain. However, numerous postal addresses which were not in the public domain were made public by the data breach. There were 207 such entries with addresses – which is not an insubstantial amount.

The manner in which the infringement became known to the Commissioner

87. The infringement became known to the Commissioner as a result of the Cabinet Office submitting a Personal Data Breach Report to the ICO within 72 hours of becoming aware of the data breach in accordance with Article 33(1) of the GDPR.

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

88. Not applicable.

Adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42

89. Not applicable.

Aggravating and mitigating factors

90. Beyond the matters referred to above there were no other significant factors that aggravate or mitigate the infringement.

Deterrent Effect

91. The Cabinet Office is a long-established organisation at the heart of government that processes a variety of data across a range of activities. It has the standing, access to resource and expertise, and sophistication to provide a high standard of organisational and technical measures in comparison to, for example, a small private sector organisation or a small public authority. Organisations that have the means to do so, are expected to take the most stringent possible preventative measures. The Cabinet Office would have incurred very little, if any, cost in implementing a procedure that could have prevented the data breach.

92. Further, the honours list is an annual process involving high profile and vulnerable individuals. The Cabinet Office should have been more aware of the need for strong security arrangements. Following an external review initiated by the Cabinet Office, cultural challenges were identified in regard to data protection requirements.

93. For the avoidance of doubt, the Cabinet Office has not been held to a higher standard than another like controller, merely a high standard in relation to an important and high-profile processing activity undertaken by it. The Cabinet Office has the standing, access to resource and expertise, and sophistication to provide a high standard of organisational and technical measures. The penalty reflects the Cabinet Office's breach when considered in that context, albeit some reduction has been made to the penalty to reflect the Cabinet Office's representations with regard to deterrent effect.

Reducing the amount to reflect any mitigating factors, including ability to pay

94. The Commissioner is not aware of any financial hardships or factors that would reduce the Cabinet Office's ability to pay. Whilst the Response to the Notice of Intent refers to the current strain on public finances including as a result of the Covid-19 pandemic, no specific figures or details were provided in relation to the extent of any such strain or hardship on the Cabinet Office. Nor does the Commissioner consider there are any other factors that should lead to a reduction in the penalty amount.

95. The spending and budget of the Cabinet Office was previously understood to be in excess of £1 billion in 2019/20. However, in the Response to the Notice of Intent, the Cabinet Office stated that the appropriate budget amount was £381 million. The Commissioner accepts that £381 million is the appropriate budget figure. For the avoidance of doubt, the Cabinet Office's spending/budget has not been used in any sort of mechanistic fashion to determine the penalty amount. Rather it was considered that the Cabinet Office is of sufficient size to be able to withstand the proposed penalty. This position holds true even on the basis of the Cabinet Office's budget being £381 million.

96. Taking into account all of the above, the Commissioner is of the view that a penalty in the sum of £500,000 is effective, proportionate and dissuasive.

Summary and decided penalty

97. For the reasons set out above, the Commissioner has decided to impose a financial penalty on the Cabinet Office.

98. Taking into account all of the factors set out above, the Commissioner has decided to impose a penalty in the amount of **£500,000 (five hundred thousand pounds)**.

Payment of the penalty

99. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by 14 December 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.

100. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

(a) the imposition of the monetary penalty and/or;

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

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

102. Information about appeals is set out in Annex 1.

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

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

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

- period for appealing against the monetary penalty and any variation of it has expired.

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

Dated the 15th day of November 2021

.....

Elizabeth Denham
Information Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 55B(5) of the Data Protection Act 1998 gives any person upon whom a monetary penalty 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:e

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:e

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 monetary 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 (Information Rights) are contained in section 55B(5) of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).