DATA PROTECTION ACT 2018
(PART 6, SECTION 149)

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE

To: The Crown Prosecution Service

Of: 102 Petty France, London, SW1H 9EA

1. The Crown Prosecution Service ("**CPS**") is a "controller" as variously defined in sections 3(6) and 32 of the Data Protection Act 2018 ("DPA 2018"). The CPS prosecutes criminal cases that have been investigated by the police and other investigative organisations in England and Wales.

2. The Information Commissioner ("**the Commissioner**") hereby issues CPS with an Enforcement Notice under section 149 DPA 2018. The Notice is in relation to a contravention of the sixth data protection principle set out in section 40 DPA 2018. This Notice would accordingly be issued under section 149(2)(a) DPA 2018.

3. This Notice explains the Commissioner's decision to take enforcement action. The specific steps that CPS is required to take are set out in Annex 1.

4. The Commissioner has previously served CPS with a Preliminary Enforcement Notice ("the PEN") dated 4th July 2023. CPS provided its written representations ("the Representations") in response to the PEN on 26th July 2023. The Commissioner has taken into account the entirety of the Representations when deciding to issue

this Notice and refers to the Representations below when appropriate.

Legal framework for this Notice

5. DPA 2018 contains various enforcement powers in Part 6, which are exercisable by the Commissioner.

6. Section 149 DPA 2018 materially provides:

"(1) Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person—

(a) to take steps specified in the notice, or
(b) to refrain from taking steps specified in the notice,

or both (and see also sections 150 and 151).

(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 2 of Part 3 … of this Act (principles of processing);

…

(6) An enforcement notice given in reliance on subsection (2), (3) or (5) may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure."

7. Section 150 DPA 2018 materially provides:

"(1) An enforcement notice must—

(a) state what the person has failed or is failing to do, and

(b) give the Commissioner's reasons for reaching that opinion.

(2) In deciding whether to give an enforcement notice in reliance on section 149(2), the Commissioner must consider whether the failure has caused or is likely to cause any person damage or distress.

…

(4) An enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with (but see the restrictions in subsections (6) to (8)).”

8. By reason of section 34(3) DPA 2018, the controller shall be responsible for, and to be able to demonstrate compliance with the sixth data protection principle in section 40 DPA 2018.

Background

9. On 18th March 2018 a CPS [redacted] ("[redacted]") copied a CPS case file case concerning historic child abuse from a CPS computer system onto an unencrypted personal USB device. The [redacted] did this with the intention of passing the device to a colleague who would be dealing with the case. Therefore, the [redacted] used the USB device for CPS business and for the discharge of his employment duties. As such, at all material times the [redacted] was acting on behalf of CPS.

10. The Representations challenged the Commissioner's finding that the [redacted] used the USB device for CPS business and for the discharge of his employment duties, due to the [redacted] purportedly contravening the CPS Electronic Media Policy that was in force at the relevant time and because the [redacted] purportedly acted on his own volition and not in discharge of his employment duties, because there was no requirement for him to provide the case file to his colleague who had similar access rights to the CPS computer system and who would therefore have been able to access it via their own account/device.

11. There is nothing in the Representations that cause the Commissioner to alter his findings in paragraph 9 and not to proceed with this Notice. When initially downloading the material to the portable media device in performing his actions, the [redacted] accessed the information as part of his role and his actions were not of a nature that break the usual responsibility that a controller has for its employees – the individual was initially seeking to provide information to a colleague for a legitimate business purpose. The Commissioner has considered the CPS Investigation Report written by [redacted] which supports the Commissioner's findings in this regard. For example, The Investigation Report expressed the finding at paragraph 5.2 that "*I do not believe that [the [redacted]'s] intentions went beyond a desire to share material with another [redacted] in a manner convenient to himself to help in the presentation and preparation of the case*." Furthermore, there is no evidence that the [redacted] was aware of the CPS' Electronic Media Policy or trained on it.

12. The Commissioner is not satisfied that there were appropriate technical or organisational measures in place to prevent the [redacted] from downloading sensitive data to a portable media device, or that

there was sufficient awareness of controller's expectations of the [redacted] in this regard. As the [redacted] had been erroneously included in an Active Directory Group, encryption software had not been downloaded to the individual's device, meaning that data was able to be downloaded to a self-procured USB without protections such as a means of preventing the USB's ability to access / download material, or by the presence of encryption software.

13. For the avoidance of doubt, the USB device that the [redacted] copied the case file to was not provided for their use by CPS. Instead, the USB device was provisioned by the [redacted] themself and belonged to them. For the purpose of this Enforcement Notice, the provisioning of the USB device by the [redacted] is referred to as "self-procurement".

14. For the further avoidance of doubt, despite having a policy in place, it was clear in response to the Commissioner's enquires that the self-procurement of USB devices by CPS staff for use on CPS business was a practice that CPS was aware of but was not rigorously controlled through appropriate technical measures which would have reduced the prospect of a breach of this nature.

15. The Representations challenged the finding referring to the Electronic Media Policy, but there is nothing within the Representations that cause the Commissioner to alter his findings and to proceed with this Notice. The Commissioner refers to the audit that is identified at paragraph 34(IV) below and the information provided by the CPS in response to the Commissioner's investigation.

16. The documents that were copied to the USB device included medical and social care records of the complainant in the case; police records including the incident log and investigation reports;

the record of interview of the defendant; witness names and addresses; instructions to the [redacted] and related case information; and other sensitive documents. These documents contained personal data, including personal data of the highest sensitivity, the processing of which is regulated by Part 3 DPA 2018. The personal data related to approximately ten persons.

17. None of the documents containing the personal data were encrypted when stored on the USB device.

18. The documents were held by CPS for the purposes of the prosecution of a criminal offence or offences, the trial of which took place after the coming into force of DPA 2018 on 25 May 2018 ("the commencement date" for the Act). The processing of at least some of these documents constituted "sensitive processing" within the meaning of section 35 DPA 2018.

19. For the purposes of Part 3 DPA 2018, CPS is a "competent authority" within the meaning of section 30. Part 3 applied to the processing of the personal data within the documents from the commencement date. Prior to the commencement date, the processing was regulated by the Data Protection Act 1998 ("DPA 1998").

20. The [redacted] did not hand-over possession of the USB device to their colleague, but instead retained possession of it with the CPS documents stored thereon, until a precise date that is unknown to the Commissioner, but is believed on the balance of probabilities to have been in August 2018, when the [redacted] gave possession of the USB device to their [redacted], so that the [redacted] could load onto it a [redacted] video.

21. The trial of the case to which the documents and personal data related commenced on [redacted] and concluded later that month with the conviction of the defendant.

22. On 27 November 2018 the [redacted]s [redacted] made contact with the [redacted] about the USB device, having viewed some of the documents.

23. The [redacted] returned the USB device to the [redacted] on 28 November 2018. The [redacted] informed their manager at CPS of the incident on 29 November 2018 and handed-in the USB device. Thereafter, CPS commenced an investigation and reported the incident as a personal data breach to the Commissioner on 4 December 2018. CPS also communicated the fact of the breach to the impacted persons.

24. Following the reporting of the breach, the Commissioner commenced an investigation. The investigation found that:

I. The [redacted] was wrongly included in an Active Directory group of approximately 1,500 persons, which gave him the ability to download a large volume of sensitive personal data to his personal, unencrypted USB device, without appropriate controls being in place.
II. Some members of the Active Directory group were able to use USB devices without the forced installation and use of CPS encryption software.
III. The CPS did not provide USB devices for its staff to use, but instead allowed a system of self-procurement of these devices by staff.
IV. The use of self-procured USB devices was not subject to supervision by CPS or asset management.

V. CPS considered that it would be a "considerable exercise" to ascertain how many members of the Active Directory group were included in error, so it could not provide the Commissioner with this information, nor could it confirm how long people had been members of the group for.

VI. CPS considered that the management of portable media was "complex", which resulted in a far greater disparity than CPS would have expected between the number of users that had write access to data and the numbers that had licences to use encryption software. Of the approximately 1,500 members of the Active Directory group, only 800 had access to CPS encryption software. Therefore, it seems likely that not every member of the Active Directory group who had the capability to copy or download data to USB drives were able to encrypt such data.

25. The Representations challenged the accuracy of the information now contained in 24.I. above. The Commissioner accepts that due to the approach adopted for the use of gender pronouns in the PEN, there was a potential for it to convey a different meaning to the one intended and the Commissioner's understanding of the evidence. Paragraph 24.I conveys the Commissioner's understanding and there is nothing in the Representations that causes him to alter his findings and not proceed with this Notice.

26. The Representations also challenged the Commissioner's findings now contained in paragraph 24.III, adopting the challenge made to paragraph 14. As such, there is nothing in the Representations to cause the Commissioner to alter his findings and not proceed with this Notice.

27. The Representations also challenged the Commissioner's findings in paragraph 24.IV, adopting the challenge made to paragraph 14. The Representations also claimed that the CPS understood the importance of maintaining a comprehensive records of all approved use of USBs. However, during the course of the investigation, the CPS was asked about whether it maintained an asset register for USB devices. In response, the CPS stated that "USBs are not held on the register" and that "Asset Registers do not include USB devices". The CPS also stated, in response to a question about self-procured USBs, that "due to this limited usage and only being available should other methods not be suitable, it is not appropriate per se to include them on an asset register, as they are immediately, after use, sent outside the organisation". As such, there is nothing in the Representations to cause the Commissioner to alter his findings and not to proceed with this.

The contravention

28. The Commissioner has concluded that the retention of the documents on the USB device by the [redacted] between 25 May 2018 and August 2018, followed by the passing of possession of the USB device with the documents stored thereon to the [redacted]'s [redacted] followed by the viewing of some of the contents on the device by the [redacted] constituted a personal data breach within the meaning of section 33 DPA 2018.

29. Furthermore, the Commissioner is of the view that the sixth data protection principle in section 40 DPA 2018 was contravened, due to a failure of CPS to implement appropriate technical and organisational measures for the security of personal data.

30. Section 40 materially provides:

"The sixth data protection principle is that personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, "appropriate security" includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)."

31. Moreover, the Commissioner notes the requirements of section 66(1) DPA 2018, which materially provides:

"(1) Each controller and each processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks arising from the processing of personal data."

32. The Commissioner is of the view that section 40 was contravened, for the following reasons:

I. CPS did not implement appropriate technical and organisational measures for the management of the Active Directory group, in that the [redacted] was included in the Active Directory group in error, with the result that they had permission to access and write personal data that they were not entitled to. Furthermore, CPS was unable to provide an account of the extent of this problem, with the result that the Commissioner considers it likely that other persons were wrongly given access and write permissions to which they were not entitled, or did not need.

II. CPS did not implement appropriate technical and organisational measures for the provisioning and use of

portable media storage devices, in that due to it being aware of the use of self-procured USBs and due to its failure to implement appropriate countermeasures to manage the risks involved in their use it allowed the [redacted] to self-procure and use USB devices for the storage and transportation of highly sensitive personal data in a manner that was free of any form of formal asset control by CPS, including registration of assets and recording of their use. To all intents and purposes, the processing of the data on the [redacted]'s USB device was wholly ungoverned and free of supervision by CPS and had it not been for the responsible conduct of the [redacted] CPS would have remained unaware of the fact that a personal data breach had occurred. In light of the foregoing, CPS did not implement appropriate technical and organisational measures to prevent, detect or respond to a personal data breach.

III. CPS did not implement appropriate technical and organisational measures for the encryption of highly sensitive personal data that were stored on the USB device.

33. The Commissioner is also of the view that CPS' position that it would be a "considerable exercise" to ascertain how many members of the Active Directory group were included in error and its position that the management of portable media was "complex", which resulted in a far greater disparity between the number of users that had write access to data and the numbers that had licences to use encryption software than CPS would have expected, is further evidence of a failure to implement appropriate technical and organisational measures for the security of personal data.

Issue of the Notice

34. The Commissioner considers that the contravention of DPA 2018 is a significant one that warrants enforcement action. His reasons for this conclusion include the following.

I. The personal data that were put at risk were of the highest sensitivity.

II. Due to the absence of appropriate technical and organisational measures, the personal data breach would have gone undetected but for the actions of a member of the public.

III. The measures that should have been adopted for asset control and encryption are basic controls for the use of portable storage media.

IV. CPS has rejected both the Commissioner's 2019 Audit recommendation that it should procure portable media such as USB drives for use by its staff, instead of allowing self-procurement by staff, and the recommendation that records should be kept of their distribution, ownership and use.

V. Without enforcement action, the risks to personal data arising from the self-procurement of USB devices by CPS personnel, which are illuminated by the personal data breach, will be unremedied.

VI. The contravention was longstanding and pre-dated the commencement date of DPA 2018.

VII. Since this incident, the CPS has reported further incidents to the ICO involving the loss of portable storage devices. The ICO therefore consider there to be an on-going issue with the use of such devices which needs to be addressed.

35. The Representations challenged the information that is now contained in paragraph 34.III, by repeating the Representations made in challenge to paragraph 24.IV. As such, they do not cause

the Commissioner to alter his findings and not proceed with this Notice.

36. The Representations challenged the information that is now contained in paragraph 34.IV, by stating the rationale for the rejection of the Audit recommendations. The Commissioner relies on that rationale in support of his findings and so the Representations do not cause him to alter them and not proceed with this Notice.

37. The Representations challenged the information in the PEN that is contained in paragraph 34.V, by repeating the Representations made in challenge to paragraph 14. As such, they do not cause the Commissioner to alter his findings and not proceed with this Notice.

38. The Commissioner therefore requires CPS to take the steps set out in Annex 1.

39. The Commissioner considered, as he is required to do under section 150(2) DPA 2018 when deciding whether to serve an Enforcement Notice, whether any contravention has caused or is likely to cause any person damage or distress. The Commissioner considers that there was clear potential for distress to have been suffered by the impacted data subjects, due to the overall context of the case and the nature of the data involved.

40. Moreover, CPS has also recognised that the personal data breach may have caused significant emotional distress to those data subjects.

41. However, the Commissioner considers that compliance with the provisions of DPA 2018 referred to above to be a matter of central importance to data protection law. Even if a failure to comply has not, or is not likely, to cause any person damage or distress, the issue of this Enforcement Notice to compel compliance would nonetheless be an appropriate exercise of the Commissioner's enforcement powers.

42. The Commissioner has considered whether it is practicable for CPS to comply with the requirements of Annex 1. In this regard the Commissioner notes that the requirements are basic ones for the procurement, use and tracking of portable data storage media and they are proportionate to the facts in issue in this case.

43. Having regard to the significant nature of the contravention, the scale of the personal data being processed and the context in which it is processed, the Commissioner considers that this Enforcement Notice is a proportionate regulatory step to bring CPS into compliance.

44. The Commissioner has also had regard to the desirability of promoting economic growth, and the potential impact his Notice might have. The Commissioner considers the proposed enforcement action is unlikely to have an impact on any measure of economic activity or growth in the UK.

Terms of the Notice

45. The Commissioner therefore exercises his powers under section 149 DPA 2018 to serve an Enforcement Notice requiring CPS to take specified steps to comply with the DPA 2018. The terms of the proposed Notice are set out in Annex 1 of this Notice.

Consequences of failing to comply with an Enforcement Notice.

46. If a person fails to comply with an Enforcement Notice the Commissioner may serve a penalty notice on that person under section 155(1)(b) DPA requiring payment of an amount up to £17,500,000 or 4% of an undertaking's total annual worldwide turnover whichever is the higher.

Right of appeal

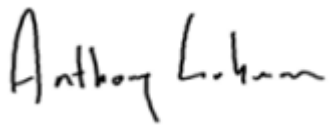
47. By virtue of section 162(l)(c) DPA there is a right of appeal against this Notice to the First-tier Tribunal (Information Rights). If an appeal is brought against this Notice, it need not be complied with pending determination or withdrawal of that appeal. Information about the appeals process may be obtained from:

General Regulatory Chamber
HM Courts & Tribunals Service
PO Box 9300
Leicester
LE1 8DJ
Telephone: 0203 936 8963
Email: grc@justice.gov.uk

48. Any Notice of Appeal should be served on the Tribunal within 28 calendar days of the date on which this Notice is sent.

Dated the 20th day of December 2023

Signed:



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

ANNEX 1

TERMS OF THE ENFORCEMENT NOTICE

By no later than 3 months of issue of the notice CPS shall take the following steps:

1. Implement appropriate technical and organisational measures to prohibit and prevent the use by CPS personnel of self-procured USB portable storage devices for the storage, transportation and related processing of personal data of which CPS is the controller.
2. Implement appropriate technical and organisational measures to provision the use of CPS-procured USB portable storage devices by CPS personnel for the storage, transportation and related processing of personal data of which CPS is the controller.
3. Implement appropriate technical and organisational measures for the purposes of asset management of CPS-procured USB portable storage devices, including the registration of the procurement of these assets, requests for use of these assets, distribution of these assets, sharing of these assets with third parties, such as law enforcement agencies and the courts, and the timely return of these assets.
4. Implement appropriate technical and organisational measures to ensure that the use of CPS-procured USB portable storage devices complies with CPS policies and procedures for data protection, including security principles and the implementation of measures such as device or file encryption.
5. Implement appropriate technical and organisational measures to limit the use of CPS-procured USB portable storage devices, taking account of the overall risks of their use, the context of processing and the presence of available alternatives to their use such as

secure file transfer using the Egress solution or related solutions approved by the National Cyber Security Centre.