From: David Martindale [redacted]
Sent: Thursday, February 8, 2024 10:33 AM
To: Elaine Angus <Elaine.Angus@ico.org.uk>
Subject: RE: Email from ICO - INV/0375/2023

External: This email originated outside the ICO.
Hi Elaine

With apologies again for the delay please find attached our response to your letter dated 19 January.
I acknowledge however the oversight in us sending this out to you which means you are only receiving it today - 8 February 2024.

Kind regards
David

David Martindale
Data Protection Officer & Head of Information Management
Undercover Policing Inquiry (UCPI)
Mob: [redacted]

From: David Martindale [redacted]
Sent: 08 January 2024 12:28
To: Elaine Angus
Subject: RE: Email from ICO - INV/0375/2023

External: This email originated outside the ICO.
Dear Elaine

Thank you. I conform receipt and note the requested response date of 23 January.

Kind regards

David Martindale
Data Protection Officer & Head of Information Management
Undercover Policing Inquiry (UCPI)
Mob: [redacted]

From: David Martindale [redacted]
Sent: Tuesday, February 6, 2024 2:22 PM
To: Elaine Angus <Elaine.Angus@ico.org.uk>
Subject: RE: Email from ICO - INV/0375/2023

External: This email originated outside the ICO.
Yes definitely, and possibly by this afternoon. I am tracking down where the final version got to.

David

From: David Martindale [redacted]
Sent: Tuesday, February 6, 2024 2:11 PM
To: Elaine Angus <Elaine.Angus@ico.org.uk>
Subject: RE: Email from ICO - INV/0375/2023

External: This email originated outside the ICO.
Dear Elaine

I do apologise, it is my first day back from a period of 3 weeks' leave today. I drafted and shared a response with colleagues internally in January, before I went away. Once cleared there seems to have been an oversight in this being set out to you while I was on leave. This is now urgently being looked into this afternoon and I am sorry for the delay.

Kind regards
David

David Martindale
Data Protection Officer & Head of Information Management
Undercover Policing Inquiry (UCPI)
Mob: [redacted]

UNDERCOVER POLICING INQUIRY
PO Box 71230
London NW1W 7QH

Official - Sensitive

David Martindale
Information & Security Manager
Undercover Policing Inquiry

✉ [redacted]

www.ucpi.org.uk

@ucpinquiry

Ms Elaine Angus
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

By email only: Elaine.Angus@ico.org.uk

19 January 2024

Dear Ms Angus

Re: Case Reference Number INV/0375/2023 (previous reference IC275909-V8K9)

I am writing in response to your emailed correspondence dated 8 January 2024 and have addressed the questions contained within.

Firstly, the Undercover Policing Inquiry (UCPI) would like to assure the Information Commissioner that significant steps have been taken to manage this security breach and we have implemented a range of enhanced security protocols to address any previous shortcomings.

In order to assist with your investigation and provide the information you are seeking I have re-listed your numbered questions below in chronological order and provided our responses to each of these. We have also had significant engagement with our Sponsorship Department, the Home Office, during the course of this investigation and have taken their lead in addressing many areas which required attention.

The SD cards and information contained on them.

1. You have stated that the two SD cards contained government data classified as secret from closed legal hearings. Is this still your understanding?

It is our understanding that only one SD card contained a 45-minute extract of an extension of time hearing. The second SD card has since been identified as being blank.

2. Please clarify do the SD cards hold recordings of the closed hearings and/or associated documents? Please explain.

As above. The SD cards are used as a means of transferring the recordings made on a recordable device to our secure IT system. There is no need to retain the audio transcript on them once this process has been completed and the audio from each SD card is subsequently deleted.

3. You have explained that the SD cards were not returned to the locked safe. What date were the SD cards last in the organisation's possession and accounted for?

The date of when the two SD cards were lost cannot be determined due to the lack of auditable records. An internal investigation suggests that the SD cards were last seen on 28 September 2023.

Do you know when the SD cards were last taken out of the safe (if they were ever in the safe)?

No, as above. An internal investigation suggests that the SD cards were last seen on 28 September 2023.

5. Please can you clarify are the SD cards linked in some way? For example, do they involve the same individuals or legal hearing that took place on the same day etc?

No, the SD cards are not linked. The second SD card was blank.

6. Please provide a view as to whether it is likely the cards went missing at the same time.

That cannot be determined due to the lack of auditable record keeping. An internal investigation suggests that the SD cards were last seen on 28 September 2023

7. What was the status or purpose of the SD cards, were they working copies, originals, a back-up etc. Please explain.

The SD card held an original recording taken on 27 September 2023; it was approximately 13 minutes long and concerned an extension of time application; there is nothing on the recording which could be considered capable of damaging national security if made public and the missing data was not capable of identifying the officer and/or their partner.

8. Please describe the physical and technical security measures that were in place to store and protect the cards. For example, the safe was in a keypad protected room and the SD cards were password protected.

[redacted]

9. Please provide specific details regarding the nature and amount of personal data compromised as a result of this incident.

There are references to an unnamed individual through use of his undercover name which included details of the approximate area he lived in and some limited information regarding his domestic circumstances. It is not now considered capable of damaging national security if made public and the missing data was not capable of identifying the officer and/ or their partner.

The incident

10. You have stated that you became aware that the cards were unaccounted for on 5 December 2023 and that they were unaccounted for since 22 November. Can you clarify that the date is 22 November 2023 and clarify how do you know this is the date? For example, do you know they were taken out of the safe on this date and do you have records that show this?

The date of when the two SD cards were lost cannot be determined due to the lack of auditable records. An internal investigation suggests that the SD cards were last seen on 28 September 2023.

11. You have stated that you are unable to identify the staff members involved. I assume you mean that you cannot identify the individuals who last had possession of the cards and who should have put them in the safe. Should the safe records or whatever system you had in place have shown this? Please confirm did the SD cards go missing from the safe or did they never actually get put into the safe at all?

Following further investigation, we have been able to narrow down the SD card movements to three individual staff members who handled the SD card. However, despite internal and independent investigation we are currently unable to identify the individual who last handled the SD card. The safe system in operation would not have shown this and that policy has since been changed. We cannot say if they went missing from the safe.

Policies and procedures

12. You have stated that everyone involved knew these SD cards containing this security classification of data had to be stored in a specified safe in the office. You have confirmed that security inductions cover this. Please provide a bit more information about this. Are the security inductions provided to all UCPI staff, is it at induction into the organisation, is it refreshed at any point etc? If this induction/awareness is in writing, please provide a copy of the relevant slide/section as it would have been on the date the SD cards became unaccounted for.

The security induction covers the need for S classified information to be stored in a safe instead of a standard filing cabinet, which is used for information classified at OFFICIAL. The inductions are provided to all new staff and have been for several years. They form part of the new starters induction pack and our guidance is that refresher training is re-issued each year. Attached is a copy of this induction which does not specify the type of media, only the security classification of the data. The removable media policy has been updated and circulated to reflect enhanced handling. This is being supported by briefing sessions to more fully communicate individual and unit responsibilities.

13. Other than the security inductions please explain if there is any other way the UCPI ensured that the staff would have known that the SD cards needed storing in the safe.

See above. There was a policy in place which has now been updated to take account of SD cards and recent events. There is an understanding among colleagues of what is required for this classification of information.

14. As the data controller, did the organisation have a policy (or policies), written procedure or guidance which set out how data of this type should be handled prior to the incident? If so, did the circumstances of this particular incident breach this policy? Please provide a copy of any relevant written policy or procedure and describe any relevant policy or procedure which is not documented.

There was an existing general policy but not specific processes in place. Internal and independent assurance exercises undertaken after the data breach have identified the need for an assurance process with a tracking system which covers the handling and storage requirements of this classification of data.

15. You have stated that internal process guides and protocols will now be revised to be clearer. Please clarify what has changed within the protocols and either provide a highlighted copy or describe the changes.

There is now a dedicated removable media policy, see enclosed. Also see the explanation below in response to question 25.

16. Please confirm that the organisation permits the use of portable or removable devices eg SD cards etc, only where these are issued by its own IT department and, if so, whether these are detailed on an asset register or subject to regular audits. Please also confirm that any such devices are encrypted to current industry standards, if that is the case, and how compliance with these measures is enforced. Potential harms/harms

Yes, they were always issued by the IT department and there have now been arrangements made to encrypt them to industry standards and to list and account for them on an asset register, which is subject to audit controls. Previous accreditation had not required us to encrypt these cards for internal use.

17. Thank you for confirming in your email of 12 December 2023 that the main security concern relating to a risk to national security has been eliminated and that the relevant document was not present on the missing SD cards. Just to clarify initially you stated that one assessment was that wrongful disclosure in relation to one matter is 'significant and capable of damaging national security if made public'. Am I correct to understand that this is no longer the case?

Yes, that is correct – answer 18 provides further detail.

18. You have stated that that the loss of the data is likely to result in a high risk to data subjects. Please explain in depth what personal data is contained on the cards and why it is considered high risk?

Following further investigation, it was identified that one SD card contained details of an unnamed individual, the approximate area where he lived and some limited domestic details. The other is believed to be blank. It is our view that this is no longer categorised as 'high risk'. To a member of the public this information would not make personal identification possible. The initial high-risk assessment was made based on potential specific information being released which was capable of more readily identifying an individual.

19. Has the organisation received a formal complaint from any individual affected by this breach? If so, please provide details.

No. A formal complaint from the individual affected has not been received. The incident has been reported to the legal representative of the individual concerned and they are conducting their own risk assessment.

20. Is there any evidence to date that the personal data involved in this incident has been inappropriately accessed/processed? If so, please provide details.

No. There is no evidence that data involved in this incident has been inappropriately accessed/processed.

21. Is the data contained on the SD discs lost to the enquiry (ie are they the only copies)? If so, please describe the impact of this. For example, will the hearing need to be held again etc?

No, it has been retained. The SD cards are a mechanism to upload audio recording to our secure systems. This recording has been uploaded and checked on our secure IT system. The other SD card was blank.

Remedial Actions and Other

22. Have the police been informed?

The relevant branch of the Metropolitan Service who is legally representing this individual has been informed.

23. Have you told the individuals who are affected by the breach? If so, when did you tell them and how did you tell them?

The Metropolitan Police legal representatives of the individual have been informed, so they could decide whether to inform their client.

24. Please provide a copy of any internal security incident report (with personal data redacted) that may have been produced in connection with this incident.

See attached.

25. What further action has been taken to minimise the possibility of a repeat of such an incident?

We have been working closely with the Inquiry sponsor, independent accreditors and security specialists to development and implement a programme to significantly improve our security process, policy and assurance frameworks. This work is being taken forward through a security improvement action plan.

26. Had the UCPI produced a Data Protection Impact Assessment (DPIA) in relation to the processing of this type of personal data (ie information from closed hearings)? If so, please provide a copy of the DPIA.

This is currently being checked, we do have some DPIAs for our data categories.

Yours sincerely

David Martindale
Data Protection Officer & Information Security Manager