Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

[redacted]
Crown Prosecution Service
8th Floor, 102 Petty France
London
SW1H 9EA

By email only to: [redacted]

12 August 2022

Dear [redacted]

Case Reference Numbers: INV/0438/2020
INV/1612/2020
INV/0237/2021

I write to inform you that the ICO has now completed its investigation into three separate incidents involving the loss of personal data.

INV/0438/2020

In summary, it is my understanding that on 17 December 2019 a wallet containing two unencrypted Victim Recorded Interview (VRI) discs was sent back from Lincoln Crown Court to the Crown Prosecution Service (CPS) East Midlands' Area Office after a trial was aborted. The discs were transferred back from court to the CPS offices by an approved CPS courier, in a lockable case, however the discs were not booked back into the CPS office and are considered lost. The discs contain visual and audio recordings of police interviews of [redacted] victims of sexual assault.

INV/1612/2020

In summary, it is my understanding that on 25 November 2020 the CPS North East office discovered that a hard copy case file, relating to an alleged rape, could not be located; the loss was discovered when attempts were made to locate the file in preparation for trial proceedings in December 2020. The file's last recorded location was on the collection racking within the CPS room at Newcastle Crown Court on 04 December 2019, where it had been placed for collection and return to CPS offices. Whilst the CPS believe that the file was returned to CPS offices and incorrectly destroyed, there is no record of the file's return to CPS premises.

In summary, it is my understanding that [redacted] requested a sexual offences case file in January 2021. Following the [redacted] request the CPS made attempts to find the file but has not been able to locate it. It is understood that the [redacted] had previously been sent the file on 20 May 2015 and that they have a record that the file was returned to CPS on 06 June 2017 via tracked DX delivery service, however CPS has no record that the file arrived back at CPS premises.

All three of the above cases have been considered under the Data Protection Act 2018 (the DPA 2018) due to the nature of the processing involved.

Our consideration of these cases

We have investigated whether CPS has complied with the requirements of the data protection legislation.

In the course of our investigations we have noted that the data involved in each case was sensitive and the loss of this data therefore had the potential to cause substantial distress to the affected data subjects; however it is understood that no actual detriment appears to have been caused to the affected data subjects as a result of these incidents. It is also noted that the loss of the data does not appear to have affected any related court proceedings.

At the time of the incident it is understood that some procedures were in place in respect of records management and logging the movements of files and removable media, however, it is noted that such procedures do not always appear to have been documented at the time of the incidents. It is also noted that the policies and guidance in place at the time of the incident do not appear to provide sufficiently clear guidance in respect of the logging and transfer of data involved in these incidents.

We have also considered and welcome the remedial steps taken by CPS in light of this incident. In particular we note that searches have been undertaken to try to locate the lost files and CDs, risk assessments were undertaken by Police to assess the potential impact on data subjects and consideration was given and affected data subjects were notified of the incidents where deemed appropriate.

However, after careful consideration and based on the information provided, we have decided to issue CPS with a reprimand in accordance with Schedule 13 (2) of the DPA 2018.

The reprimand has been issued in respect of the following processing operations that have infringed the DPA 2018:

- Section 40 which states that 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)."

In particular, in each case CPS did not have a suitable end-to-end logging process in operation to adequately record the movements, to, from and within CPS offices, of case files and removable media containing personal and special category data. In failing to have a logging process in place to record such movements this had contributed to the loss of files and CDs containing personal and special category data, which had the potential to cause distress to affected data subjects.

Further Action Recommended

The Commissioner recommends that CPS could take certain steps to improve its compliance with DPA2018. In particular:

1. If not already completed, take steps to ensure an appropriate logging process is implemented to record end-to-end movements and handling of files and removable media to, from and within CPS offices, including recording destruction;

2. Take steps to raise staff awareness of the end-to-end logging process, including providing staff with sufficient documented guidance explaining what the process is and how such logging is expected to be conducted;

3. Take steps to monitor and review logs at regular intervals to ensure all recorded files and removable media are accounted for.

Whilst the above measures are suggestions, I would like to point out that if further information relating to this subject comes to light, or if any further incidents or complaints are reported to us, we will revisit this matter and further formal regulatory action may be considered as a result.

https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and new powers under the UK GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely

[redacted]
Lead Case Officer
Civil Investigations
Regulatory Supervision Service
The Information Commissioner's Office
[redacted]

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the United Kingdom General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes basic details about the complaints, investigations and self-reported data breaches it handles. These details include the name of the organisation concerned, the dates that we opened and closed the case, and the

(https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

We do not include personal data in the published datasets and will anonymise the names of sole traders etc prior to publication. We also do not publish cases concerning domestic CCTV complaints and may not publish certain other cases if we feel it is not appropriate to do so in the circumstances.

If you wish to raise an objection to us publishing a case in the datasets, whether or not we have published it yet, please contact us explaining your reasons for this at accessicoinformation@ico.org.uk .

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice