Upholding information rights

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

[redacted]
Data Protection Officer
North Yorkshire Police

By email only to: [redacted]

02 November 2022

Dear [redacted]

Case Reference Number: INV/0413/2020

I write to inform you that the ICO has now completed its investigation into North Yorkshire Police's (NYP) incident where information was processed inaccurately, resulting in the wrongful arrest of the data subject.

In summary, on 07 May 2019 NYP's Covert Standards processed an application submitted by NYP's Digital Forensics Unit (DFU). The application was to acquire communications data/IP (internet protocol) address resolution for a single IP address. The purpose of the application was to establish who was the user of an electronic device, which utilised a particular IP address during a specific period in 2018.

When processing the application, the Covert Standards SPoC (Single Point of Contact) inputted a date incorrectly from the application's search criteria into communications provider's portal.

This mistake resulted in the [redacted] application erroneously resolving the IP address to a device used by the data subject. Believing that the data subject had used the device during the time specified in the application, NYP arrested the data subject on 07 August 2019 for the serious offence of making indecent images of children.

At the time of the arrest, the data subject's home was searched by NYP and three electronic devices belonging to the data subject were seized. The data subject was released under investigation.

DFU discovered the mistake on 29 November 2019 and a senior manager in DFU was notified. The DFU senior manager picked the notification up on their return to work on 02 December 2019.

On 02 December 2019 having identified that a mistake had been made, NYP visited the data subject to inform them of the personal data breach and apologise for the error.

NYY attribute the cause of the breach to human error, which was compounded by the mistake not being identified as it went through various stages from Covert Standards to DFU.

The ICO noted that written guidance and (the College of Policing) training provided for the Covert Standard SPoCs advised that where possible, to utilise copy and paste from original documentation into workflow systems, to ensure consistency and elimination of transcription or manual errors. However, the search criteria in this incident was entered manually into the communications portal, which opened up the risk of key stroke errors.

NYP acknowledged that checking and peer reviews of the data returned from the application focused on the IP address and that insufficient attention was given to the time period processed.

Further, the mistake was not identified for almost four months, which meant the data subject remained under investigation and wrongfully arrested for this period for a serious offence.

In this instance, NYP were working in a highly sensitive area of undercover police work and where it is known that errors can result in significant harm, with individuals being wrongly accused of crimes. The ICO consider it is reasonable to have expected NYP to have worked to a high degree of accuracy, with high quality training given to team members. Also, that clear, stringent, and effective guidance and procedures to have been in place to ensure the accurate processing of a [redacted] application.

This case has been considered under the Data Protection Act 2018 (the DPA 2018) due to the nature of the processing involved.

For more information about our powers under the data protection legislation please see the attached leaflet.

- ICO Enforcement leaflet - UK GDPR and DPA 2018

Our consideration of this case

I have investigated whether NYP has complied with the requirements of the data protection legislation.

In the course of my investigation I have noted that upon discovery of the breach, NYP took immediate action to inform the data subject. This was done in person by a senior NYP officer and the data subject's electronic devices were returned to them.

NYP undertook a candid approach when explaining the breach to the data subject and gave them an apology. The data subject was advised of the steps being taken by NYP to correct or erase any records in relation to the incident.

NYP gave the data subject the contact details for NYP's DPO, the ICO, the Professional Standards Department and the Civil Claims Unit; therefore providing the data subject with avenues by which to either make a compliant or seek redress.

Of significant concern in this investigation were any records held by NYP relating to the wrongful arrest. It is noted that NYP have taken necessary steps to correct the data subject's record to ensure that he would not suffer any detriment in the future as result of inaccurate records.

We have also considered and welcome the remedial steps taken by NYP in light of this incident. In particular, I have noted the following:

- The employee concerned was reminded of importance of data quality and accuracy and asked to complete the [redacted] package. This was completed in December 2019.

- Training is now in place for every new SPoC that comes into the role. This was completed in August 2020.

- DFU will highlight on the front of application packages if the acquisition is for a single IP address.

- Additional peer reviews and checks have been put in place throughout the [redacted] application process.

- An additional step of when the application results are uploaded, the applicant is notified with a phone call and they will be made aware that it is just a single IP address.

- Each case involving a single IP address will be reviewed on a case-by-case basis; a Detective Inspector will provide a clear rationale for the relevant team executing the warrant as to why the warrant is necessary.

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

Details of reprimand

The reprimand has been issued to NYP in respect of the following infringements of the DPA 2018:

Part 3, Law Enforcement Processing, Chapter 2 – Principles
38 The fourth data principle

This states that:

(1) (a) personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date and

(b) every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

(4) All reasonable steps must be taken to ensure that personal data which is inaccurate, incomplete or no longer up to date is not transmitted or made available for any of the law enforcement purposes.

(5) For that purpose –

(a) the quality of personal data must be verified before transmission or made available,

(c) if, after personal data has been transmitted, it emerges that the data was incorrect or that the transmission was unlawful, the recipient must be notified without delay.

Based on the findings of this investigation, the ICO considers that NYP did not take reasonable steps to ensure there was adequate checking / peer reviews in place for the latter part of the [redacted] application process. This is a direct infringement of Section 38 (1)(a) and (b) and (4) of Part 3, Chapter 2 of the DPA 18.

Further, the ICO considers that NYP did not verify the personal data before it was made available for law enforcement purposes. Nor did it rectify the personal data or notify the data subject without delay (in this respect the ICO refers to the length

of time it took for NYP to identify the mistake). This is a direct infringement of Section 38 (5) (a) and (b) of Part 3, Chapter 2 of the DPA 18.

Further Action Recommended

The Commissioner recommends that NYP could take certain steps to improve its compliance with DPA 2018:

1. Stronger emphasis should be given to the importance of accuracy in any written guidance and internal training for IP address resolution. In particular, when detailing the steps for entering the search criteria data into the communications provider's portal and when double checking the search criteria processed (highlighting that **all** elements of the search criteria should be checked).

2. Review policies and procedures with a view to adhering to the strategies and best practice directions as suggested by the College of Police training and the IPCO Error Reduction Strategy (ERS) guidance. In particular, that where possible, to use copy / paste to ensure consistency and elimination of manual errors, and where this is not possible, a second SPOC / peer must verify the details have been inputted correctly.

3. Further, it is noted that from the IPCO ERS and College of Policing's Communications Data Single Point of Contact (CD-SPoC) training that a number of SPoC peer reviews and checks are required in the IP address resolution process. Please ensure your written guidance and internal training follow these safeguards.

4. Your policies and procedures should have prominent, sufficient and adequate practical guidance for employees in order to avoid a similar breach occurring again.

5. Take steps to test all of the new processes introduced by your organisation as a result of this incident and ensure that they are embedded in the IP address resolution procedure.

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.

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link:

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]
Investigation Officer
Investigations
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 outcome. Examples of published data sets can be found at this link (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 icoaccessinformation@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