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
Chief Constable North Yorkshire Police
Alverton Court
Crosby Road
Northallerton
North Yorkshire
DL6 1BF

By email only to: [redacted]

2 March 2022

Dear [redacted]

Case Reference Number INV/0785/2021

I write to inform you that the ICO has now completed its investigation into the breach which was reported to the ICO on 8 September 2021.

In summary, it is my understanding that on 3 July 2018 North Yorkshire Police (NYP) generated a duplicate Single Justice Procedure (SJP) for a driving offence. As a result, a data subject was convicted of the same driving offence twice.

This case has been considered under Part 3 of the Data Protection Act 2018 (the DPA 2018) due to the nature of the processing involved.

Our consideration of this case

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

In the course of my investigation I have noted that:

1. The data subject was convicted of the duplicate offence on 29 August 2018. As a result, the data subject received a second fine and was disqualified from driving due to 'totting up'.

2. The disqualification had minimal impact on the data subject in terms of the practicalities of driving as prior to the breach the data subject had decided not to renew their license. However, the data subject has suffered financial loss as a result of paying the fines and prosecution costs in relation to the

duplicate offence. It is understood that the stress caused by the breach has also exacerbated the data subject's existing eye condition and had a negative effect on their eyesight.

3. On 18 September 2018, the data subject contacted the Ministry of Justice (MoJ) to raise the issue of not being due for 'totting up'.

4. On 4 October 2018, NYP confirmed to the court that the duplicate offence was generated in error. On 5 October 2018, the order of disqualification and other penalties were removed, and the case was withdrawn.

5. On 22 December 2020, the data subject sent a letter to the MoJ raising a complaint. This complaint was received by NYP on 1 June 2021 and was responded to by NYP's Prosecution Team Manager on 17 June 2021.

6. On 18 August 2021, NYP's Civil Litigation lawyer was notified of a civil claim made by the data subject. On 31 August 2021, NYP's Civil Litigation Lawyer notified the Compliance Team of the civil claim being handled.

7. NYP reported the breach to the ICO on 8 September 2021.

We have also considered and welcome the remedial steps taken by NYP in light of this incident. In particular that there is now a documented SJP in place which contains additional steps to avoid the risk of duplicate SJPs. NYP has also made a number of improvements to its governance to ensure compliance with the data protection legislation, including the introduction of a mandatory Managing Information e-learning package.

However, 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 in respect of the following processing operations that have infringed the DPA 2018:

- Part 3, Chapter 2, Section 38 (1) which states that –
"*(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."

- Part 3, Chapter 4, Section 67 (1) which states that –
  "If a controller becomes aware of a personal data breach in relation to personal data for which the controller is responsible, the controller must notify the breach to the Commissioner
  (a) Without undue delay, and
  (b) Where feasible, not later than 72 hours after becoming aware of it."

In particular, NYP did not have suitable processes in place at the time of the incident. This is because there was no documented process in place to instruct staff to check for a duplicate before generating a new SJP.

In view that NYP is processing sensitive personal data and criminal offence data, we would reasonably expect a documented process to be in place to avoid the risk of duplicate SJPs. We would also expect NYP to provide its staff with specific data protection training to ensure that they are aware of the importance of accurately recording personal data. It is noted that prior to the breach, NYP did not provide specific training relating to the DPA 2018.

Further to this, NYP first became aware of the breach on 4 October 2018. However, multiple staff failed to notify the Compliance Team of the breach. As a result, the Compliance Team only became aware of the breach on 31 August 2021 upon notification of the civil claim being handled. This was followed by a further delay as the Compliance Team did not report the breach to the ICO until 8 September 2021. Therefore, it is evident that NYP's incident handling fell short of expectations in this instance.

Further Action Recommended

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

1. Review its data breach reporting policies and procedures to ensure that all incidents and near-misses are appropriately recorded and investigated. Lessons learnt from these incidents should also be shared with all relevant

staff members.

2. Ensure that there is sufficient regard to the issue of contingency planning within the department that deals with data protection issues. This will enable NYP to continue to meet its obligations under the legislation.

3. Ensure all employees receive and refresh data protection training on a regular basis. Training should be designed to meet the needs of colleagues at all levels, and should equip employees with the skills required for handling special category personal data and criminal offence data in line with the data protection legislation.

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. 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-theico/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
Information Commissioner's Office
Tel: [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 the outcomes of its investigations. 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/).

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