Upholding information rights

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

[redacted]
Deputy Director – Privacy/Data Protection Officer
Data Privacy and Governance Team
Justice Digital and Technology Directorate
Ministry of Justice
102 Petty France
London SW1H 9AJ

By email only to: [redacted]

26 August 2022

Dear [redacted]

ICO Case Reference Number: INV/0602/2021
MoJ Case Reference Number: MoJ 0016

I write to inform you that the ICO has now completed its investigation into the unauthorised disclosure of personal information.

In summary, it is my understanding that following the temporary closure of HM Courts & Tribunals Service (HMCTS) buildings as a result of the COVID pandemic, a bulk amendment facility was used by staff to effect the required adjournment of a significant number of Magistrates' Courts' cases. Although the bulk adjournments were primarily made during April and May 2020, it was not until late September 2020 that it became apparent that the use of the amendment facility had resulted in guilty/not guilty plea records being incorrectly recorded. In some instances, this resulted in the incorrectly recorded verdicts being automatically cascaded onto the Police National Computer (PNC).

It is noted that HMCTS is an executive agency, sponsored by the Ministry of Justice (MoJ), and that HMCTS comes under the MoJ's umbrella registration with the ICO. Therefore it is considered that the MoJ is the data controller in respect of this matter.

This case has been considered under 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 the MoJ has complied with the requirements of the data protection legislation.

In the course of my investigation I have noted that this incident arose as a result of HMCTS's response to the requirement to adjourn court cases during the national COVID pandemic and the speed with which the pandemic evolved could not reasonable have been foreseen.

A large number of data subjects were affected by the incident and HMCTS could be considered fortunate that no evidence has been provided of actual detriment suffered by data subjects as a result. It is noted that complaints were received but that these have been resolved by the way of letters of apology and no identified complaints in relation to this matter have been received by the ICO. However it is also noted that the majority of data subjects remain unaware of the unauthorised processing of their personal information and there remains the potential, therefore, for detrimental impact to have been suffered without the data subjects being aware of the cause.

We have also considered and welcome the remedial steps taken by the MoJ in light of this incident. In particular, ensuring all affected records have been corrected, ensuring that no safeguarding issues have been identified, and disabling the functionality to prevent further incidents.

However, after careful consideration and based on the information provided, we have decided to issue the MoJ 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:

- 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)."

It was stated that the ATM functionality which was used by staff in response to the adjournment requirement was introduced in February 2019 and that prior to the COVID pandemic it would have been rarely used, being described as "neither necessary, nor a commonly used function, because results can and are routinely applied to cases individually." It was also stated that its use in respect of the bulk adjournment had not been anticipated; that it was for staff to select the most suitable method of adjourning the necessary cases; but that there was no single, central directive instructing staff on how, or why, to adjourn cases. While

acknowledging that the electronic IT bulletin issued when the functionality was introduced states that it cannot be used for adjournments, this information was issued more than one year prior to the requirement for the adjournments; it was not re-issued at the time the requirement for bulk adjournments was communicated to staff nor was the potential risk separately highlighted to staff, some of whom may have joined HMCTS after the initial instruction was issued. Had adequate instruction been provided and appropriately communicated to staff it is considered likely, on the balance of probabilities, that the incident would not have occurred.

Upon identification of the root cause of the incident, it was stated that clear instructions were issued. This instruction was in the form of a staff bulletin email issued on 25 June 2020 which stated that "a number of incidents" had been raised indicating that errors had been identified by HMCTS. However instead of issuing a clear instruction to staff to cease taking specific action, to prevent the errors from continuing, the bulletin simply repeated the previously issued information and stated, "If you do not want, to copy the plea over to other cases, please do not use the ATM functionality." The email noted that no functional changes would be made to the process. This bulletin is brief and is not considered to be an informative piece of guidance. The lack of a specific instruction to staff to cease using the ATM functionality is considered to have further compounded the incident and to be a missed opportunity to have curtailed an ongoing incident.

It was noted that some Courts had correctly used the case summary sheet during the incident period, and this was evidenced by some staff contacting the IT helpdesk having noticed the errors. However the MoJ stated that the helpdesk, because ATM was working, "*did not regard these reports as IT 'incidents' or recognise the wider implications.*" In response to the errors being raised with the IT helpdesk, the ATM guidance was simply re-issued without amendment on 25 June 2020 to "*remind staff how to use ATM correctly*". The MoJ stated that a full check of the case summary sheet for cases adjourned using ATM would have revealed the incorrect copying of plea data. Therefore, if all the required checks had been undertaken for each individual case adjourned it is considered likely, on the balance of probabilities, that the errors would have been identified and thus that the automatic cascade of information to the PNC would have been prevented.

From the evidence provided, functionality existed for adequate checks on the processing of personal information to be undertaken by staff working remotely. It is of concern, given the unique circumstances of the pandemic, that HMCTS did not consider it necessary to have implemented any additional safeguards to ensure security of personal information being processed.

Evidence of HMCTS Data Incident training was provided. However, the training content is considered to be lacking in specific detail. There is no information regarding the processing that resulted in the incident under investigation included in the document. There is also no information regarding the requirement for risk assessments or Data Protection Impact Assessments to be undertaken; little reference to GDPR within the training; no reference to law enforcement processing; and no explanation that special category data requires enhanced consideration. Evidence has been provided of missed opportunities to identify the incident under investigation as being a data breach which is considered to indicate that the training provided was inadequate to have mitigated against this type of incident from occurring.

In conclusion, a reprimand is being issued due to infringements noted in respect of section 40 of the DPA 2018.

Further Action Recommended

The Commissioner recommends that the MoJ, and HMCTS, could take certain steps to improve its compliance with DPA 2018. In particular:

1. Conduct a review of guidance available to staff for all processing methodologies to ensure each contains adequate information and is fit for purpose.

2. Any areas of processing which would benefit from risk assessment, or the conducting of a Data Protection Impact Assessment should be identified, and appropriate remedial action taken.

3. Consideration should be given to the introduction of a central repository for guidance and standard operating procedures, which should only contain current versions of documents in order to staff to be certain they are referring to the most up-to-date information. Consideration should also be given to routinely sign-posting staff to this repository, and its location included in induction training.

4. Staff should be required to confirm acceptance of any newly issued or amended/updated policies and procedures. Any instances of non-compliance should be monitored, with appropriate remedial action taken.

5. The content of data protection training should be reviewed to ensure it is adequate for the purpose of fully informing staff of their responsibilities under current data protection legislation. Refresher training should be

routinely undertaken, ideally annually, with completion monitored and any instances of non-compliance promptly remediated.

6. A Data Protection Impact Assessment should be considered for the system intended to replace Digital Mark-Up to ensure that all aspects of processing have been appropriately risk assessed. Remedial measures in respect of any areas of identified weakness should be undertaken prior to processing commencing.

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]
Lead Case Officer - Civil Investigations

Regulatory Supervision Service
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 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