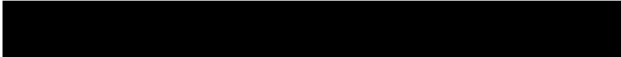




f.a.o. *Matthew Rycroft CBE*
Permanent Secretary
Office of the Secretary of State for the Home Department
Peel Building
2 Marsham Street
London SW1P 4DF

By email only to: 

05 October 2022

Dear Matthew

ICO Case Reference Number: INV/0114/2022

We write to inform you that the Information Commissioner's Office (ICO) has now completed its investigation into the breach which was reported to the ICO by the Home Office on 4 April 2022.

In summary, on 5 September 2021 an envelope containing four documents classified 'Official Sensitive' (the Documents) was found at a venue in London, by venue staff. On 6 September 2021, the venue staff handed the documents in to the police and the police subsequently handed them to the Home Office on the same day.

This case has been considered under the United Kingdom General Data Protection Regulation (the UK GDPR) due to the nature of the processing involved.

Our consideration of this case

We have investigated whether the Secretary of State for the Home Department has complied with the requirements of the data protection legislation, as the relevant Data Controller for the personal data contained within the Documents.

In the course of our investigation, we noted that the Documents included two Extremism Analysis Unit Home Office reports and two copies of one Counter Terrorism Policing report. The Documents contained personal data relating to three Data Subjects as follows:

- a foreign United Kingdom visa applicant who is the subject of the Documents, and,
- two Metropolitan Police staff.

The personal data affected included special category data.

Upon discovery of the breach, an investigation was launched by the Government Security Group in the Cabinet Office. That investigation has now concluded and we understand it found that the most likely source of the Documents was the Home Office.

We have also considered and welcome the remedial steps taken by the Secretary of State for the Home Department in light of this incident. In particular that business processes have been updated to ensure that all similar documents are given a unique reference number.

However, after careful consideration, we have decided to issue the Secretary of State for the Home Department with a reprimand in accordance with Article 58(2)(b) of the UK GDPR.

Details of reprimand

This reprimand has been issued to the Secretary of State for the Home Department, as the relevant data controller of the personal data concerned, in respect of the following infringements of the UK GDPR.

- Article 5 (1) (f) which states:

"Personal data shall be:

(f) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

- Article 33 (1) which states:

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification under this paragraph is not made within 72 hours, it shall be accompanied by reasons for the delay."

In particular the Secretary of State for the Home Department has failed to ensure an appropriate level of security of personal data, resulting in the inappropriate disclosure of personal data relating to three Data Subjects. It is noted that the

Documents were classified 'Official-Sensitive' and contained specific handling instructions. Those handling instructions stated that to ensure the confidentiality of the reports, they must be kept securely, and appropriate measures must be taken to prevent the unlawful or unauthorised processing of the personal data they contain. In this instance, the handling instructions for the reports were not followed as they were found unsecured in a venue in London where they were accessed by unauthorised individuals.

It is also noted that prior to the breach, the Secretary of State for the Home Department did not have a specific sign out process in place for the removal of 'Official-Sensitive' documents from its premises. The document designation of 'Official-Sensitive' indicates that extra care should be taken when handling such information to ensure its security. Therefore, the ICO would expect the Secretary of State for the Home Department to have a documented sign out process in place to ensure that all 'Official-Sensitive' documents containing personal data can be accounted for when taken out of the office.

In addition, staff of the Secretary of State for the Home Department first became aware of the breach on 6 September 2021, however the breach was not reported to the ICO until 4 April 2022. Although it is accepted that at the time of discovering the breach it was unclear as to how the documents came to be left at the venue, the Secretary of State for the Home Department was nevertheless aware that the incident involved Home Office reports which contained personal data and special category data. Therefore, it is our view that the Secretary of State for the Home Department had sufficient information in order to report the breach to the ICO within the statutory time limits, namely within 72 hours of first becoming aware of it.

Further Action Recommended

The Information Commissioner recommends that the Secretary of State for the Home Department take steps to improve its compliance with UK GDPR. In particular:

1. Review the handling instructions for 'Official-Sensitive' information to ensure that they are up to date and refer to the UK GDPR.
2. Ensure appropriate security of personal data in accordance with Article 5 (1)(f) of the UK GDPR. In particular, consider introducing a sign out

process for 'Official-Sensitive' documents containing personal data to ensure that this information can be accounted for when out of the office. Further information about ensuring an appropriate level of security of personal data can be found at the following link:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/>

3. Review applicable policies and procedures in accordance with Article 24 of the UK GDPR, to ensure that prominent and sufficient practical guidance is provided to staff regarding the removal of physical records, containing personal data, from Home Office premises.
4. Demonstrate compliance with the requirements of accountability in accordance with Article 5(2) of the UK GDPR. In particular, it is advisable to monitor the compliance of staff with existing procedures or policies by regular assurance testing and auditing. Further to this, we recommend that a review of all data protection training is undertaken to ensure that sufficient practical guidance is given to staff on how to comply with the legislation. Further information about accountability can be found at the following link:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/>

5. Ensure that all personal data breaches are reported to the ICO within 72 hours as stipulated by Article 33 of the UK GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of Data Subjects. The learning from any breach report analysis should also be shared across the organisation to embed lessons learnt from any breach incidents.

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/>



Information Commissioner's Office

If further information relating to this incident comes to light, or if any further incidents or complaints are reported to us, we may revisit this matter to consider whether further formal regulatory action is necessary.

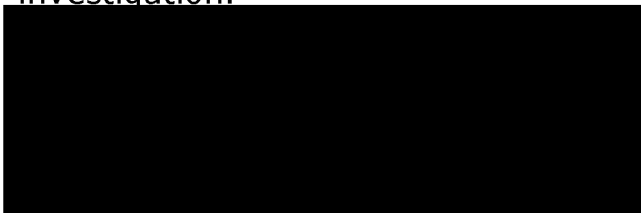
Publication Of The Reprimand

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 from it or where the case highlights a risk or novel issue.

We intend to publicise the outcome of this investigation in line 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

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



Yours sincerely,

Stephen Eckersley
Director of Investigations
Regulatory Supervision Service
The Information Commissioner's Office

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