Upholding information rights

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

[redacted]
Complaints & Investigations Analyst
Office of the DPO
Secretary of State for the Home Department (Home Office)

By email only to: [redacted]

16 August 2022

Dear [redacted]

ICO Case Reference Number: INV/0853/2021
Home Office Case Reference Number: PDBR-4659-2122

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 a Home Office employee contacted members of the public as part of the creation of an education programme for staff into the historical background and circumstances of individuals arriving into the UK which had led to the matter that became widely and collectively known as the "Windrush scandal" occurring. It is my understanding that interviews were conducted with individuals who had previously been affected by the "scandal"; that the interviews were recorded on the employee's personal mobile phone; and subsequently uploaded to her personal YouTube account, from where they were shared with other Home Office employees.

Although there are considered to be two separate elements to this matter – firstly, the unsanctioned recording of three separate face-2-face interviews and secondly, the uploading of these interviews onto social medial (YouTube) – the matters have been investigated as one overall incident.

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

Our consideration of this case

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

In the course of my investigation I have noted that the incident represented the potential for considerable detriment to be suffered to a small number of data subjects, over and above the detriment and distress already caused by the Windrush scandal as a whole. However it is noted that no formal complaints have

been received and the Home Office could therefore be considered fortunate that the actual detriment appears limited.

It is noted that the breach arose from action being undertaken by the Home Office in response to one of the recommendations made by the independent Lessons Learned Review following the Windrush scandal. Therefore, it is considered that the Home Office should have had heightened awareness of the importance of data protection compliance. This is of particular concern when considering that the failure to comply with previous data protection legislation was a significant contributory factor in the occurrence of the Windrush scandal itself.

Furthermore, prior to the incidents occurring the Home Office had been issued with an Assessment Notice in response to concerns regarding its adequate compliance with data protection legislation. It is acknowledged that the final audit report was published after the first interview took place. However awareness of data protection compliance concerns was known to the Home Office as a result of being served with the Assessment Notice and this would also have informed the Home Office that the business area involved in the incident, Immigration Enforcement, was an area of key concern for the ICO. It is considered that the Home Office's preparations for the work required in response to the Assessment Notice should, on the balance of probabilities, have resulted in a heightened awareness of, and a review of, processing activities within Immigration Enforcement and that this work should already have been ongoing prior to the employee's secondment starting.

We have also considered and welcome the remedial steps taken by the Home Office in light of this incident. In particular that an additional data protection training package, produced by members of ODPO, has been introduced.

However, after careful consideration and based on the information provided, we have decided to issue the Home Office with a reprimand in accordance with Article 58 of the UK GDPR.

Details of reprimand

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

- Article 5(1)(f) which states that personal data shall be "processed in a manner that ensures appropriate security of the 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 24(1) which states that "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

- Article 32(1)(a) and (b) which state that "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

  (a) The pseudonymisation and encryption of personal data;
  (b) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;"

From the evidence presented it is considered that inadequate organisational action has been taken to ensure compliance with data protection legislation. The data protection compliance failures are evidenced by

- no instructions were issued by the secondment department about the handling of personal information;
- no specific training was given because it was a short secondment;
- no checks were undertaken to ensure secondees were compliant with data protection training;
- no adequate oversight of work by secondees was undertaken by managers;
- no Data Protection Impact Assessment was undertaken;
- no Terms of Reference were completed;
- no privacy information was provided to interviewees.

This is considered to be evidence of breaches of articles 5(1)(f), 24(1), 32(1)(a) and 32(1)(b) of the UK GDPR.

In addition, the breach report stated that the employee informed the data subjects that the interviews she was conducting would provide awareness for Immigration Enforcement staff as a result of listening to their stories. The breach report also stated that all the data subjects were willingly interviewed and gave their consent, with another person present at the time of the interview to look after their wellbeing. However no evidence of officially recorded consent has been

provided. This is considered to be further evidence of breaches of articles 32(1)(a) and 32(1)(b) of the UK GDPR.

The Home Office stated that links to the videos saved onto the employee's personal YouTube account were shared with 26 individuals, being a mixture of Home Office employees and [redacted]. Five individuals are known to have viewed the videos on or around 23 April 2021, the day on which the first video was uploaded, with a further 10-15 individuals viewing videos between 15 and 21 September 2021. When considering that the source of the video would have been apparent to the recipients, it is of concern that none of the five individuals who viewed the first video in April 2021 raised concerns regarding data protection compliance of such personal information, which had been gathered for business purposes, being held on a personal YouTube account. It is acknowledged that the fact the employee did not consider if the conducting or recording of the interviews would represent a breach of data protection legislation could be considered an instance of individual human error. However the fact that none of the employees who viewed the recordings on YouTube raised concerns, and in the absence of any evidence that either of the employee's managers considered data protection compliance implications in respect of the interviews having been conducted, this is considered to be evidence of inadequate awareness of data protection legislation at an organisational level, rather than being limited human error. This is considered to be evidence of the failure on the part of the Home Office to have ensured its employees had an adequate awareness of their data protection responsibilities when processing personal information and represents an infringement of articles 5(1)(f) and 24(1) of the UK GDPR.

It was stated that neither of the employee's managers had realised that the videos had been created outside of Home Office IT systems. No explanation for why this was the case has been provided but considering the refusal by one manager of the employee's request for an officially provided mobile phone, it is difficult to understand how either manager believed the interviews had been officially recorded. It was stated that following identification of the incident on 16 September 2021, when the employee's managers became aware of the existence of the interview recordings on her mobile phone and also on YouTube, the Strategic Lead made internal enquiries to the Home Office's legal advice department to establish if the videos could be used and how to obtain consent. It is of concern that even at this stage the matter was not considered by either manager to potentially constitute a data breach – either in terms of the unsanctioned recording of personal information; the processing of it on the employee's personal mobile phone; or the uploading of the interview recordings onto YouTube. This is considered to be further evidence of infringements of articles 5(1)(f), 24(1), 32(1)(a) and 32(1)(b) of the UK GDPR.

Finally, the lack of easily identifiable and appropriately labelled guidance regarding employee use of personal IT equipment (including mobile phones) is considered to be an organisational failure on the part of the Home Office and an aggravating factor in this incident occurring. This is considered to be further evidence of an infringements of articles 5(1)(f) and 32(1)(b) of the UK GDPR. Furthermore, the saving by the employee of the interview recordings onto her personal YouTube account is considered to be in contravention of the scope of the Home Office's collective guidance in respect of the use of social media. This is considered to be a further infringement of Article 5(1)(f) of the UK GDPR.

In conclusion, a reprimand is being issued due to infringements noted in respect of 5(1)(f), 24(1), 32(1)(a) and 32(1)(b) of the UK GDPR.

Further Action Recommended

The Commissioner recommends that the Home Office could take certain steps to improve its compliance with UK GDPR. In particular:

1. The Home Office should ensure that the additional data protection training package produced by ODPO is rolled out across all departments as a mandatory requirement, with annual refreshment undertaken .

2. The Home Office should ensure that an adequate record of successful completion of data protection training is maintained, with clear lines of responsibility identified for ensuring instances of non-compliance are appropriately resolved.

3. Compliance with steps 1 and 2 above should be routinely monitored.

4. Undertake a review of the current guidance in respect of the identification of data protection incidents to ensure it provides employees with adequate and appropriate information with respect to the identification of such incidents.

5. The above guidance should be re-circulated with additional consideration given to further awareness raising sessions in individual business departments to mitigate against a repeat of this type of incident.

Whilst the above measures are suggestions, I would like to point out that if further information relating to this matter 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