Information Commissioner's Office

Upholding information rights

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

[redacted]

By email only to: [redacted]

4 October 2022

Dear [redacted],

Case reference number: [redacted]

I write to inform you that the ICO has now completed its investigation into [redacted] processing of both the personal and special category data of its United Kingdom (UK) staff.

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

Our consideration of this case

The investigation considered whether [redacted] processing activities from 25 May 2018 (the introduction of the UK GDPR) onwards have complied with the requirements of data protection legislation.

I have noted that, in your letter of 2 March 2022, you stated that [redacted] had not re-introduced the use of biometric readers in its venues after the extended closure caused by the COVID-19 pandemic.

[redacted] clarified that the re-opening of its venues included a re-assesment as to whether or not biometric readers were an appropriate measure, given the advances in technology of time and attendance systems, and the potential of finding a solution that did not require the processing of biometric data.

This is a welcome development, and the ICO is satisfied that, at this time, no biometric data is being processed by [redacted].

However, after careful consideration and based on the information provided, we have decided to issue [redacted] with a reprimand in accordance with Article 58 of the GDPR/Schedule 13 (2) of the DPA 2018.

Details of reprimand

To confirm, this reprimand has been issued in respect of the following processing operations that have infringed the UK GDPR:

- **Article 5(1)(a)** of the UK GDPR which states that personal data shall be "processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency)"

  In particular, [redacted] did not identify an appropriate lawful basis for the processing of special category data (SCD).

  In its response to the ICO, [redacted] stated that the processing of SCD was covered by Article 9(2)(b) which states that;

  "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject".

  ICO guidance states that examples of such processing of SCD under Article 9(2)(b) would include;

  - checking if individuals are entitled to work in the UK;
  - ensuring health, safety and welfare of employees;
  - maintaining records of statutory sick pay and maternity pay; or
  - deducting trade union subscriptions from payroll.

  Furthermore, ICO guidance states that the purpose must be to comply with employment law, or social security and social protection law; and that a data controller must be able to identify the specific legal obligation or right in

question. The condition does not cover processing purely to meet contractual employment rights or obligations.

The data controller must also be able to justify why the processing is necessary, and that it is a reasonable and proportionate way of meeting the specific legal obligation or right.

When asked what obligation under employment law made the processing necessary, [redacted] has stated it is to comply with Section 9 of the Working Time Regulations 1998 (Exhibit 1.3). Specifically, this requires employers to keep adequate records of timekeeping.

It is the ICO's view that [redacted] has not adequately demonstrated that the processing of biometric data was a necessity and did not provide sufficient justification as to why other less intrusive methods would not fully meet the needs identified.

Whilst [redacted] had stated that alternative methods for meeting the same purpose had been tried, and were found to be less effective, [redacted] did not sufficiently demonstrate why biometric data was the only effective method of achieving its purpose.

Article 9(2)(b) was not a legitimate legal basis for the processing. This is an infringement of Article 5(1)(a) as the SCD was not, therefore, processed lawfully.

- **Article 9(1)** of the UK GDPR which states that "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".

  Article 9(2) then proceeds to state "Paragraph 1 shall not apply if one of the following applies".

Subparagraphs (a) – (j) then list the conditions in which Paragraph 1 does not apply, and are referred to as the lawful bases for processing.

As stated above, the lawful basis provided by [redacted], Article 9(2)(b), was not valid. This resulted in SCD being processed, despite being prohibited by Article 9(1). This is an infringement of Article (9)(1).

- **Article 35** of the UK GDPR which states that "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

  [redacted] has confirmed that the system had been in use since 2014, but that in 2019 it decided to carry out a PIA as part of its data protection compliance processes, and in order to take a "fresh view" of the system and consider any possible improvements.

  As a result of this process, [redacted] identified what it considered to be minor improvements that could be made in order to improve transparency in relation to the use of biometric data.

  In fact, [redacted] should have carried out a Data Protection Impact Assessment (DPIA) prior to the introduction of the UK GDPR in May 2018.

  [redacted] should have been aware that the introduction of the UK GDPR made biometric processing a class of SCD, which had not been the case before. This means that any previous PIA or risk assessment would no longer be adequate, and a DPIA specific to the UK GDPR requirements was necessary.

  The responses provided by [redacted] demonstrate that no DPIA was carried out prior to the introduction of the UK GDPR to assess the risks of the biometric processing.

  This is an infringement of Article 35.

Further Action Recommended

The Commissioner is aware that [redacted] has already suspended processing of biometric processing upon the reopening of its venues, and that its potential future use is currently under review.

The ICO now requests that a DPIA be carried out by [redacted], if not already done so, before any future biometric processing is considered.

Any future biometric processing, for any purpose, should only be undertaken once a clear and valid lawful basis for that processing has been identified under Article 9.

Whilst the above measures are suggestions, I would like to point out that if further information, incidents or complaints relating to this matter come to light, we will revisit this matter and 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]
Investigations
Information Commissioner's Office
[redacted] (direct dial)

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.