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
Department for Education (DfE)
Sanctuary Buildings,
Great Smith Street,
London
SW1P 3BT

[redacted]

2 November 2022

Dear [redacted]

Case Reference Number INV/0538/2020

We write to inform you that the ICO has now completed its investigation into the sharing of personal data stored on the Learning Records Service (LRS) database, for which the DfE is the data controller. The LRS database contains both personal and special category data and at the time of the incident there were 28 million records stored on it. Some of those records would have pertained to children aged 14 and over.

The DfE permitted third party access to the LRS database outside of the DfE and subsequent processing took place of some of that personal data (including children) for the purposes of age verification, without appropriate control or oversight. The investigation has found that therefore the personal data on the LRS database was processed in an insecure manner and for purposes that were not initially intended. Furthermore, the DfE failed to be transparent about that processing.

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

Our consideration of this case

We have investigated whether the DfE has complied with the requirements of the data protection legislation.

Key Compliance Issues

The investigation found that the DfE did not comply with the following requirements of the GDPR:

Article 5 (1)(a): - 'lawfulness, fairness and transparency'
Article 5 (1)(f): - 'integrity and confidentiality'

This is because the DfE processed personal data without appropriate controls in place to sufficiently manage the risks that processing presented.

- The DfE failed to protect against the unauthorised processing by third parties of data held on the LRS database for reasons other than the provision of educational services. Data subjects were unaware of the processing and could not object or otherwise withdraw from this processing therefore the DfE failed to process the data fairly and lawfully in accordance with Article 5 (1)(a).

- The DfE failed to have appropriate oversight to protect against unauthorised processing of personal data held on the LRS database and has also failed to ensure its confidentiality in accordance with article 5 (1)(f).

In keeping with the ICO's Regulatory Action Policy (RAP), the ICO considered issuing a fine of £10,030,000 (UK Sterling). This amount was considered to be effective, proportionate and dissuasive. However, due to a revised approach by the Commissioner to the public sector, a reprimand will be issued in accordance with Article 58 of the GDPR.

For more information about the revised approach please see: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/open-letter-from-uk-information-commissioner-john-edwards-to-public-authorities/

Details of reprimand

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

- **Article 5 (1)(a)** requires personal data to be 'processed lawfully, fairly and in a transparent manner in relation to the data subject.'

  Based on the findings of this investigation, the ICO deems that the DfE has failed to process personal data fairly, lawfully and transparently. The personal data stored on the LRS database was shared with third parties and further processed without an appropriate lawful basis and without the data subject's awareness.

- **Article 5 (1)(f):** requires personal data 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 of damage, using appropriate technical or organisational measure 'integrity and confidentiality'.

  Based on the findings of this investigation, the ICO deems that the DfE failed to have adequate measures in place to prevent unauthorised or unlawful access to the LRS database.

Further Action Required

At the time of the incident the DfE were subject to a compulsory audit which took place in February 2020 following issue of an Assessment Notice. This audit did not arise as a consequence of this incident. It should be noted that the DfE has cooperated with the ICO and has been working through numerous recommendations made as a result of the audit.

It is acknowledged that access to the LRS database that was granted to the third party involved in this incident, has been permanently removed by the DfE, which has prevented further unauthorised sharing.

The investigation found no regular checks were carried out on a user's activities which left the LRS database vulnerable to misuse.

The ICO audit and the DfE themselves identified weaknesses with its registration process; and steps have been taken to strengthen these processes with the introduction of more stringent checks and controls. This enhanced process has been applied to all organisations since February 2020 and includes;

- strengthening the registration process to include more verification steps and checking an Awarding Organisation's accreditation;
- users will be required to provide an estimate of the number of learners per annum;
- users will be required to select the reason for access from a defined list rather than writing free text;
- the LRS registration form has been updated to include details of the DfE's recourse in the event of a breach of their terms and conditions;
- checks are now routinely run to identify excessive use and to de-register organisations who no longer use the LRS service.

The ICO recognises that a number of internal reviews have taken place following this incident and the ICO audit. However, The Commissioner considers that the DfE could continue to improve its compliance with the UK GDPR. The DfE is required to implement the following five measures to improve its compliance:

1) The DfE must take steps to improve transparency around the processing of the LRS database so Data Subjects are aware and are able to exercise their Data Subject rights, in order to satisfy the requirements of article 5 (1)(a) of the UK GDPR.
2) The DfE should continue to review all internal security procedures on a regular basis to identify any additional preventative measures that can be implemented. This would reduce the risk of a recurrence to this type of incident and assist compliance with article 5 (1)(f) of the UK GDPR.
3) In addition, the DfE should ensure all relevant staff are made aware of any changes to processes as a result of this incident, by effective communication and by providing clear guidance.
4) In order to improve compliance with article 36 of the UK GDPR - Prior consultation and article 35 of the UK GDPR – Data Protection Impact Assessment (DPIA), when processing personal data that is likely to result in a high risk to individuals, the DfE should complete a thorough and detailed Data Protection Impact Assessment (DPIA), which adequately assesses the risk posed by that processing. This will enable the DfE to identify and mitigate the data protection risks of that processing on individuals.
5) Further, the DfE should continue to ensure sufficient data protection training is provided to all staff. For further advice please see Training and awareness | ICO

Normally, the ICO would expect the DfE to provide an update on the steps taken after a three month period. However, due to the ongoing engagement with the ICO's Assurance Department, updates can be provided during that regular ongoing correspondence within this time scale.

It must be emphasised that the ICO's decision to issue a reprimand in this case does not detract from the seriousness of this incident, and has been reached due to a revised approach by the Commissioner to the public sector.

We 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]
Investigation Officer
Civil 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 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