Upholding information rights

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

[redacted]
Principal Information Governance Officer
Corporate Information Governance Team
The Council of the City of Wakefield (Wakefield Council)
County Hall
Bond Street
Wakefield
West Yorkshire WF1 2QW

By email only to: infosec@wakefield.gov.uk

22 September 2022

Dear [redacted]

ICO Case Reference Number: INV/0113/2022

I write to inform you that the ICO has now completed its investigation into the breach which was reported to the ICO by Wakefield Council (the Council) on 10 March 2022.

In summary, on 3 March 2022 the Council sent papers prepared as a Court bundle, in relation to Child Protection Legal Proceedings, to the parents of the child in question. The Court documents contained a Child Protection Medical Report which included the home address of the mother and her two children.

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

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

In the course of my investigation, I have noted that the mother is fearful of the father due to a history of ongoing domestic violence and a break in to a previous accommodation. Therefore, the father did not and should not know the mothers home address. As a result of the breach, the mother and her children had to be moved into emergency alternative accommodation on the same day of the breach.

The Council's internal investigation determined that the cause of the breach was a failure by the Social Worker to identify that the mothers address was included

in the Child Protection Medical Report. The Social Worker sent the documents to the Team Manager, who subsequently sent them to the Legal department. The Legal department then filed the documents to all parties of the proceedings, which included the father.

We have also considered and welcome the remedial steps taken by the Council in light of this incident. In particular that on 17 May 2022 the Council created a guide for workers which provides guidance to staff on how to use the 'hide' function and redact confidential addresses on the Children's Services system. It is also noted that a new mandatory question was added to the system on 17 May 2022 which asks Team Managers to check that confidential information has been redacted from forms.

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

Details of reprimand

The reprimand has been issued to the Council in respect of the following infringements of the UK GDPR:

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

"1. 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 24 (1) which states:

"1. 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."

In particular the Council 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 also noted that prior to the breach, the Council did not have any documented policies, procedures or guidance in place for Social Workers on how to prepare Court documents or redact confidential addresses on the Children's Services system using the 'hide' function.

Further Action Recommended

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

1. Review and update your Data Protection training documentation to ensure that it refers to the UK GDPR.

2. 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 need to redact confidential information from Court documents and how to do this.

3. 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 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/

4. Ensure the learning from any breach report analysis is shared across the organisation, not just the departments where breaches have occurred, to embed lessons learnt from any breach incidents.

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.

It is also noted that the ICO carried out a data protection audit of the Council with its consent in 2021 and that a follow up with the Council is currently planned for November 2022.

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
The Information Commissioner's Office
Direct Dial: [redacted]

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