

DATA PROTECTION ACT 2018 AND UK GENERAL DATA PROTECTION REGULATION

REPRIMAND

TO: London Borough of Hammersmith & Fulham

**OF: Hammersmith Town Hall, King Street, Hammersmith, London,
W6 9JU**

1. The reprimand

- 1.1 The Information Commissioner (the Commissioner) issues a reprimand to the London Borough of Hammersmith & Fulham Council (the Council) in accordance with Article 58(2)(b) of the UK General Data Protection Regulation (UK GDPR) in respect of certain alleged infringements of UK GDPR.
- 1.2 The Commissioner decided to issue a reprimand to the Council in respect of the following infringements of the UK GDPR:
 - i. Article 5(1)(f) of UK GDPR 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')".
 - ii. Article 5(2) of UK GDPR which states that the "controller should be responsible for and be able to demonstrate compliance ('accountability')".
 - iii. Article 24(1) of UK GDPR which states that "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".
 - iv. Article 32(1) of UK GDPR which states that "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".

2. Background

- 2.1 The Council is a local authority in West London.
- 2.2 The infringements occurred as a result of the disclosure of 'hidden' personal data in a spreadsheet (the FOI response) prepared by the Council in response to a Freedom of Information (FOI) request.
- 2.3 The FOI request to the Council was made by the requestor via WhatDoTheyKnow.com (WDTK). WDTK is a platform which is run and maintained by the civil society not for profit group 'mySociety'.
- 2.4 The FOI response contained a series of 35 hidden workbooks and the personal data was contained within areas of 10 of these workbooks.
- 2.5 It was not intended for the FOI response to contain the hidden data and the personal data was not identified prior to the FOI response being released and published by both the Council and WDTK.

3. The Commissioner's findings

Article 5(1)(f) Article 5(2) Article 24(1) Article 32(1)

- 3.1 The reasons for the Commissioner's provisional findings are set out below.
- 3.2 On 07 October 2021 the Council's response to the FOI request was published on its disclosures log on its website and the Council also provided the FOI response to the requestor via their WDTK constructed email address.
- 3.3 On 11 December 2021, WDTK published the FOI response on their website.
- 3.4 On 20 November 2023, WDTK notified the Council that WDTK had identified personal data was contained within the FOI response.
- 3.5 WDTK and the Council removed the FOI response from their websites upon discovery of the incident.
- 3.6 The incident affected a total of 6,528 individuals. Of which, 4,187 were adults and 2,342 were children.
- 3.7 The adult data subjects were employees, ex-employees and agency staff who worked or had worked for the Council. The personal data disclosed in this respect was in relation to their employment and their contact details in professional capacity. A small amount of this personal data was special category data.

- 3.8 However, the personal data belonging to the children was sensitive in nature. This data related to the placement of looked after children under the Council's care. Children's personal data is considered particularly sensitive and deserving of specific protection.
- 3.9 Of particular concern in this group of children, was the personal data belonging to 96 Unaccompanied Asylum-Seeking Children (UASC).
- 3.10 Whilst it was not apparent that the FOI response contained hidden data, anyone with knowledge of Excel would know how to inspect an Excel spreadsheet for hidden data and therefore could then access the personal data.
- 3.11 However, there is no evidence that the personal data has been inappropriately accessed, process or shared.
- 3.12 The Commissioner particularly noted the following factors with this breach:
- i. The length of the duration of the contravention.
 - ii. The large number of data subjects affected.
 - iii. Vulnerable and sensitive personal data belonging to children was disclosed.
- 3.13 The Commissioner found that the Council was unable to demonstrate its compliance with the requirements of Article 5(1)(f) Article(5)(2), Article 24(1), Article 32(1) of UK GDPR. In this respect, the Commissioner noted that the Council:
- i. Did not have specific written guidance in place for employees on how to use Excel safely for disclosing information in response to a FOI request.
 - ii. Did not have specific training to assist employees on how to use Excel safely for FOI responses.
 - iii. Did not instruct employees on how to check for hidden data in Excel spreadsheets before release or disclosure. In particular, the Council did not direct employees to use the 'Inspect Workbook' tool in Excel to check for hidden data, or that they should convert an Excel spreadsheet to Comma-Separated Values (CSV) format before disclosure.

- iv. Did not have adequate technical and organisational measures in place to ensure that the FOI response was checked for hidden data before disclosure.
- i. Did not implement best practice directions in accordance with guidance published by ICO in June 2018 [How to disclose information safely](#). This guidance discussed in detail the various ways in which electronic files can contain hidden data and how to check for hidden data. It suggested that the document inspector tool is used to identify hidden data. The guidance also suggested that a solution to problem of hidden data fields in Excel was to export data into a simple text format, such as CSV.

3.14 It is therefore Commissioner's assessment that the Council did not have adequate or appropriate technical and organisational measures in place to ensure the security of the data it was processing, and to prevent a breach such as this.

3.15 In order to achieve compliance with Articles 5(1)(f), (5)(2), 24(1) and 32(1)(b) of UK GDPR, the Commissioner would have expected the Council:

- ii. To have considered the risks of using spreadsheets to disclose information before the practice was adopted. Particularly as an Excel spreadsheet could potentially contain significant amounts of hidden or unexpected data.
- iii. To have referred to any relevant guidance from the ICO and included it in the Council's consideration of any potential risks. Further, the Council should have considered implementing any best practice guidance published by the ICO.
- iv. To have identified the potential for human error when using Excel spreadsheets in this way and to have put appropriate measures in place to mitigate this risk.
- v. To have put specific training in place for any employees using Excel for processing information requests. In this case, the Council relied on training, which was intended for other areas of work, with the general topic of redactions included.
- vi. To have issued employees with written guidance on the use of Excel for processing information requests. In particular, the Council was unable to demonstrate that it directed its

employees to use the 'Inspect Workbook' tool prior to disclosure.

3.16 In conclusion, the Commissioner has determined that the Council did not implement adequate and appropriate measures in accordance with UK GDPR when it adopted the practice of using Excel spreadsheets for FOI responses.

4. Mitigating factors

4.1 In the course of the investigation it was noted that:

- i. No copies of the personal data from the FOI response were found to be available via the internet based on searches undertaken by the Council's cyber incident response partners.
- ii. The likelihood of a third party accessing the websites and discovering the hidden data and then taking the steps necessary to access xml data hidden in the spreadsheet was considered low by the Council.
- iii. The personal data was almost three years old when it was included in the FOI response. It is likely that some of the data was out of date at the time of disclosure.
- iv. There is no evidence to suggest that the personal data has been inappropriately accessed, processed, or shared.
- v. There is no evidence that any individual has suffered any harm or detriment as a result of this breach.
- vi. There is mandatory data protection and information security training in place for all of the Council's employees.

5. Remedial steps taken by the Council

5.1 The Commissioner has also considered and welcomes the remedial steps taken by the Council in the light of this incident.

5.2 Of particular note are the following actions taken by the Council:

- i. Redaction and disclosure guidance for spreadsheets has been updated and shared with all staff via the all-staff email distribution newsletter, the Council's intranet, and casework system.

- ii. Training has been completed with the relevant team to cover the disclosure of information and the appropriate formats for disclosure.
- iii. The relevant team has updated its process so that only CSV formats will be accepted ahead of disclosure.

6. Decision to issue a reprimand

- 6.1 Taking into account all the circumstances of this case, including the mitigating factors and remedial steps, the Commissioner has decided to issue a reprimand to the Council in relation to the alleged infringements of Articles 5(1)(f), 5(2), 24(1) and 32(1)(b) of UK GDPR as set out above.
- 6.2 The Council were invited to provide representations. On 02 May 2025 the Council notified the ICO that it did not intend to make any representations.

7. Further action recommended

- 7.1 The Commissioner has set out below certain recommendations which may assist the Council in rectifying the infringements outlined in this reprimand and ensuring the Council's future compliance with the UK GDPR.
- 7.2 Please note that these recommendations do not form part of the reprimand and are not legally binding directions. As such, any decision by the Council to follow these recommendations is voluntary and a commercial decision for the Council. For the avoidance of doubt, the Council is of course required to comply with its obligations under the law.
- 7.3 If in the future the ICO has grounds to suspect that the Council is not complying with data protection law, any failure by the Council to rectify the infringements set out in this reprimand (which could be done by following the Commissioner's recommendations or taking alternative appropriate steps) may be taken into account as an aggravating factor in deciding whether to take enforcement action - see page 11 of the Regulatory Action Policy [Regulatory Action Policy](#) and Article 83(2)(i) of the UK GDPR.
- 7.4 The Commissioner recommends that the Council should consider taking certain steps to improve its compliance with Articles 5(1)(f), (5)(2), 24(1) and 32(1)(b) of UK GDPR:

- i. Review the guidance published by the ICO on 28 September 2023 'Information Commissioner's Office – Advisory note to public authorities' [Information Commissioner's Office - Advisory note to public authorities | ICO](#) and consider if there any further remedial measures the Council could implement in light of this guidance.
- ii. Consider implementing the use of ICO checklist for public authorities [disclosure-checklist-v1 0.docx](#) when preparing information from Excel for disclosure.
- iii. Consider making a mandatory requirement that material prepared for disclosure is reviewed by a peer or manager before release. Quality assurance checks, such as a mandatory peer or manager review, would be appropriate to ensure the security of the data being processed when using spreadsheets for disclosures.
- iv. Ensure that the review of the Council's online training, with the intention of updating them to detail the risks involving spreadsheets, is completed.
- v. Ensure that the Council use training to embed with its staff the correct methods for using spreadsheets, the requirements to check for hidden data and how to check for hidden data.
- vi. Revised or updated guidance and training should be underpinned by the Council in appropriate and relevant policies, and with refresher training for all relevant staff.
- vii. If it has not already done so, the Council should also ensure that any policies, guidance, or training in relation to its FOI process handling are revised and updated accordingly.

Dated 16 May 2025