Upholding information rights

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

Department for Work and Pensions
Caxton House
Tothill Street
London
SW1H 9NA

By email only to: [redacted]

31 October 2022

Dear [redacted]

Case Reference Number INV/0797/2021

I write to inform you that the ICO has now completed its investigation into the inappropriate disclosure of individuals personal data by Child Maintenance Appeals (CM Appeals) within the Department for Work and Pensions (DWP).

In summary, it is my understanding that DWP implemented the Xerox Reprographics application into CM Appeals to handle and redact CM Appeals bundles. No testing or data protection impact assessment (DPIA) was completed before implementing the application into CM Appeals. This is because DWP did not consider it necessary due to the application already being used in other service areas of DWP (such as Personal Independent Payment (PIP) Appeals). However, the redaction requirements for CM appeals are different from the other service areas the application was already implemented in. As such, the redaction functionality of the application was not tested to confirm it was compatible with CM Appeals. This resulted in CM Appeals bundles being sent to individuals unredacted, resulting in the personal data of 16 data subjects being inappropriately disclosed to third parties.

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 DWP has complied with the requirements of the data protection legislation.

In the course of my investigation I have noted that DWP did not conduct appropriate testing on the Xerox Reprographics application before implementing it into CM Appeals. I have found that the Xerox Reprographics application was not compatible with the Bundle Builder (BB) application CM Appeals already used to put together and redact CM Appeals bundles. This resulted in the redactions

made on the online versions of the bundles not being applied to the printed versions sent out to individuals. I have found that DWP, at the time of implementing the Xerox Reprographics application into CM Appeals, were of the view that testing the application before implementation was not necessary due to the application already being implemented in other service areas such as PIP Appeals. However, during the course of this investigation I have found that the other service areas the application was implemented in did not have the same redaction requirements as CM Appeal. For example, in PIP Appeals rather than redacting small sections of information from a document, it would remove the whole page from the bundle by marking it on the application as harmful. It has been explained that this was not possible to do in CM Appeals as full documents could not be removed from the bundle. Therefore, CM Appeals require the ability to redact small sections of information from bundles which was not tested before the implementation of the Xerox Reprographics application into the service area. This in turn resulted in the inappropriate disclosure of 16 data subjects personal data to third parties. This included the address of a data subject to their ex-partner with a history of domestic violence.

I have also found during this investigation that this personal data breach was not reported to the ICO within 72 hours of DWP being made aware of the issue. I have found that an affected data subject informed DWP of the personal data breach on 24 August 2021. DWP were further made aware of the incident on 4 September 2021. On 7 September 2021, the personal data breach was referred to DWPs data protection officer (DPO) team who conducted a further investigation into the incident. The personal data breach was later reported to the ICO on 10 September 2021. Considering the above, I have found that DWP have not complied with Article 33 of the UK GDPR.

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

Details of reprimand

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

- **Article 5(1)(f)**

  This 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 32(1)(b) & (d)**

  This states 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:

  b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

  d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.'

- **Article 33(1)**

  This states that ' In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.'

In particular, we are of the view that DWP have been negligent in ensuring the security and the confidentiality of the personal data it processes in CM Appeals. This is because appropriate testing was not conducted on Xerox Reprographics applications before being implemented to manage CM Appeal bundles. It was found that the applications redaction functions were not compatible with the needs and requirements of CM appeals. This is because the redactions applied to the electronic appeals bundles were not applied to the printed versions which are sent out to data subjects. This resulted in the personal data of 16 data subjects being inappropriately disclosed to third parties. We therefore consider DWP have not complied with Article 5(1)(f) of the UK GDPR.

Article 32 of the UK GDPR requires organisations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by their processing; to include the potential impacts these risks may have on the rights and freedoms of natural persons.

Specifically, Article 32(1)(b) requires organisations to implement measures that ensure the ongoing confidentiality, integrity, availability and resilience of their processing systems and services. DWP as the biggest public service department and the data controller of millions of customers personal data within the UK should have appropriately considered the potential risks associated with failure to ensure the ongoing confidentiality of the personal data it processes. This should have been considered when implementing a new application into a service area where the redaction functions had not been fully tested for compatibility.

Article 32(1)(d) requires organisations to regularly test, assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of processing. In this case DWP did not test the effectiveness of the Xerox Reprographics application before implementing into CM appeals. The applications redaction functionality was not tested prior to implementation to determine if it was compatible with CM Appeals needs and requirements. We consider that if appropriate testing was conducted prior to the applications implementation, DWP would have likely identified the root cause of this personal data breach before it occurred. As such, we are of the view that DWP have not complied with Article 32(1)(b) & (d) of the UK GDPR.

In conclusion, a reprimand is being issued due to infringements noted in respect of Article 5(1)(f), Article 32(1)(b) & (d) and Article 33(1) of the UK GDPR.

Further Action Recommended

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

1. In order to ensure ongoing compliance with Article 5(1)(f) and Article 32(1)(b) & (d) of the UK GDPR DWP should appropriately test all applications it implements into any service area before the application is used to handle/process personal data, and complete a DPIA if appropriate.

2. To ensure continuing compliance with Article 33 of the UK GDPR, DWP should review its policies and processes around reporting potential data breaches to ensure that all incidents are appropriately recorded and investigated in a timely manner.

3. Further to the above, to ensure ongoing compliance with Article 33 of the UK GDPR DWP should ensure that any future appropriate incidents are reported to the ICO within 72 hours.

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.

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
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 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