Upholding information rights

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

The Information Commissioner's response to the Department for Work and Pensions' consultation on modernising and improving their Child Maintenance service

About the ICO

The Information Commissioner has responsibility for promoting and enforcing the UK General Data Protection Regulation ('UK GDPR'), the Data Protection Act 2018 ('DPA'), the Freedom of Information Act 2000 ('FOIA'), the Environmental Information Regulations 2004 ('EIR') and the Privacy and Electronic Communications Regulations 2003 ('PECR'). She is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where she can, and taking appropriate action where the law is broken.

Introduction

The Information Commissioner's Office (ICO) welcomes the opportunity to respond to this Department for Work and Pensions (DWP) consultation on the proposed changes being made to the Child Maintenance service (CMS). In particular, the ICO acknowledges how digitising aspects of the CMS will help to modernise the service and improve the experience of those using it. The Commissioner supports such processing, provided it is carried out in compliance with data protection legislation, which will minimise harm to data subjects and enhance public trust and confidence in how their data is used, particularly by public authorities.

This response focuses on the areas of the consultation that fall within the ICO's remit, including the processing of unearned income data, expanding the list of organisations required to comply with information requests and digitising CMS notifications.

Legislative consultation

The consultation proposes legislative changes aimed at modernising and improving the current service. Therefore, under Article 36(4) of the UK GDPR, DWP will need to consult with the ICO during the preparation of these legislative proposals.

Article 36(4) requires government departments and relevant public sector organisations to formally consult with the ICO during the preparation of policy proposals for statutory or legislative measures that relate to the processing of personal data.

DCMS have produced guidance on the application of Article 36(4)[1].

Data Protection Impact Assessments (DPIA)

A DPIA is a tool that can be used by controllers to identify and minimise data protection risks to individuals. As outlined under Article 35 of the UK GDPR, controllers are required to undertake a DPIA where processing is likely to result in a high risk to the rights and freedoms of individuals. The ICO has produced guidance that outlines how DPIAs should be undertaken, and when they are legally required[2].

Article 35(3) sets out three types of processing which always require a DPIA. There are also European guidelines[3] to help controllers identify other high risk processing. As required by Article 35(4), the ICO has published a list of operations that require a DPIA, which compliments and further specifies the criteria referred to in the European guidelines. Some of these operations require a DPIA automatically, and some only when they occur in combination with one of the other items, or any of the criteria in the European guidelines.

One of the operations under Article 35(4) that automatically requires a DPIA is the matching, combining or comparing of data from multiple sources. Sections 83-89 of the consultation proposes expanding the list of organisations required to comply with information requests under regulation 4 of the Child Support Information Regulations. The consultation lists the purposes of such information requests, which include tracing the paying parent and calculating maintenance. From the description in the consultation, it appears achieving the listed purposes will require matching, combining or comparing the requested datasets from different sources, and as such, falls within scope of the aforementioned processing operation under Article 35(4). It is therefore likely that a DPIA will need to be undertaken before this processing is carried out.

[1] Guidance on the application of Article 36(4) of the General Data Protection Regulations (GDPR)
[2] Data protection impact assessments | ICO
[3] European guidelines on DPIAs and determining whether processing is likely to result in high risk

If a high risk to data subjects is identified through a DPIA, which cannot be sufficiently mitigated, the controller must consult with the ICO under Article 36(1) of the UK GDPR prior to the high risk element of the processing being carried out. The ICO will give written advice within 8 weeks, or 14 weeks in complex cases.

Data minimisation and accuracy

Sections 32-41 and 83-89 of the consultation suggests requesting a specific category of data from HMRC as well as mandating the provision of data, upon request, from other organisations including private pension providers. In accordance with the data minimisation principle under Article 5(1)(c) of the UK GDPR, the data being requested and processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

For example, the proposals include accessing and processing unearned income data from HMRC for the purpose of ensuring the child maintenance calculation more accurately reflects the income sources of the paying parents. Article 5(1)(c) requires that personal data must be limited to what is necessary in relation to the purpose for which it is being processed. This means that in order to justify the use of unearned income data, the controller should first consider alternative, less intrusive solutions and is able to justify that the inclusion of such data is necessary, proportionate and not excessive. This is equally applicable to any other HMRC data used to calculate liabilities, as well as the data that DWP propose mandating the provision of from other organisations for purposes listed within the consultation, including tracing the paying parent. DWP must only request the minimum datasets necessary to achieve these stated purposes.

The ICO welcomes the desire to process data in a way that results in a more accurate calculation of the paying parent's income. This aligns with the accuracy principle under Article 5(1)(d) of the UK GDPR which requires that data remains accurate and up to date.

Aspects of the consultation appear to propose processing less data than under the current process. For example, under the current process, in order to provide their projected/estimated annual taxable profit, newly self-employed paying parents are required to provide business plans used to secure loans or grants, profit and loss accounts and a statement of projected taxable profit. The proposal is to limit the data processed by accepting just a statement of the paying parent's projected profit. If the same objective can be achieved whilst processing

less data, this appears to align with the data minimisation principle, as data must be limited to what is necessary for the stated purposes.

However, data minimisation also requires that data be 'adequate', meaning the controller must be satisfied that the data requested is sufficient to fulfil the stated purpose. Furthermore, in accordance with Article 5(1)(d), the DWP should carefully consider if such statements accurately reflect their estimated income for the remainder of the tax year, as calculations based on inaccurate data could adversely impact the amount of child maintenance the parent with care receives. Considerations regarding these two aspects of data minimisation and the accuracy principle should be carefully balanced to ensure processing is fair and proportionate to both parents.

Similar considerations should be given to other statements the DWP is proposing to accept, such as replacing the provision of a bankruptcy/insolvency notice, amongst other pieces of evidence, with a declaration that the paying parent is no longer trading.

Transparency information

Transparency is a key component of fairness as well as a legal requirement under Article 5(1)(a) of the UK GDPR. Clear and comprehensive information on how personal data will be processed, known as 'privacy information', needs to be provided to data subjects prior to the processing taking place.

The requirement to provide privacy information is also a fundamental right under Articles 13 and 14 of the UK GDPR, which specifically list what information must be provided, depending on whether data has been collected directly from the data subject or elsewhere. This is known as the right to be informed which the ICO has produced guidance on, in order to assist controllers with their obligations[4]. This guidance lists what categories of information must be provided, in what situation and how.

It is likely that existing privacy notices (PN), known in DWP as a personal information charter (PIC), will need to be updated to take account of the additional categories of personal data obtained and the source of the data, as detailed in the consultation. The consultation proposes the processing of unearned income data, in addition to other HMRC data used to calculate liabilities, as well as further information from the expanded list of organisations

[4] Right to be informed | ICO

obligated to provide information. In the latter case, the consultation does not detail what categories of personal data are being obtained from these organisations, but such privacy information must be provided to data subjects, possibly within a PN or PIC. Such a PN or PIC should also be updated to reflect the source of the personal data, the categories of which are detailed within section 87 of the consultation and include private pension providers and companies that offer, promote or sell investment management services or facilitate share trading.

Controllers are also required to specify the recipients or categories of recipients of personal data. As such, the aforementioned organisations will need to update the privacy information they provide to take account of their obligation to provide information, upon request, to DWP.

Section 82 of the consultation explains that DWP plan to send communications via a digital method to employers and 'third parties'. It is not clear if these third parties are the organisations obligated to respond to information requests, or are separate. The ICO welcomes clarification in this respect. In any case, if personal data is being sent via this digital communication the recipients, or categories of recipients of this data will need to be specified within privacy information, as just stating 'third parties' is unlikely to be sufficient.

It is also often effective to provide privacy information using a combination of different techniques including dashboards, layering and just-in-time notices. More information on such techniques can be found in the ICO's detailed guidance.[5]

Data retention

Sections 32-41 and 83-89 of the consultation notes the processing of further categories of personal data, as already discussed in this response. The processing of such data will be subject to the storage limitation principle under Article 5(1)(e) of the UK GDPR which specifies that data must not be held for longer than is necessary in relation to the purpose for which it is processed.

Retaining data for longer than is necessary increases the risk that such data will become inaccurate, excessive, irrelevant or otherwise out of date, which may breach the data minimisation and accuracy principles. It also runs the risk that such data will be used in error.

[5] The right to be informed | ICO

Another consideration to take into account is that personal data held for too long will, by definition, be unnecessary. Most lawful bases under Article 6 of the UK GDPR require that processing be necessary for a specific purpose, meaning there is unlikely to be a valid lawful basis under which to process unnecessary data. This would result in a breach of the lawfulness provision of Article 5(1)(a) of the GDPR.

To reduce such risks it is important to ensure that data is erased or anonymised when it is no longer needed. As such, it is important that any existing appropriate retention policy is updated to take account of the new categories of data that will be processed as part of these proposals. It is important to review retention polices for each category of personal data at regularly intervals, as appropriate in the context of the processing. The ICO has produced guidance to assist controllers with determining their retention periods.[6]

Digitising CMS notifications

Section 73-82 of the consultation proposes sending, receiving and accessing CMS notifications digitally via the pre-existing online service, 'My Child Maintenance Case'. As noted above, the ICO supports the improvement and modernisation of services through further digitisation, provided it is carried out in a secure manner that complies with data protection legislation. In particular, the ICO recognises the holistic approach DWP have taken in this instance by acknowledging that an online service may not be an appropriate channel for all users, such as vulnerable customers. The ICO welcomes the proposal for the CMS to have flexibility to communicate with customers through their preferred method, which includes retaining the postal service.

The consultation does not appear to detail exactly how customers will be able to express their preferred method of communication. The ICO notes letters that previously would have been sent via post will be uploaded to the online service, after which customers will receive a SMS or email notifying them of this. It is not clear from the consultation how customers who would prefer to retain postal communication will be able to raise this prior to the digitisation of notifications, or if they will have to opt-out after the fact. However, the ICO recognises that the process may have already been considered, as the proposals are seeking to give flexibility to the CMS to meet the needs of vulnerable customers and their preferred method of communication.

[6] Principle (e): Storage limitation | ICO

When uploading letters to the online service, and when sending out subsequent notifications, personal data must be stored, transmitted and accessed in a secure manner. The integrity and confidentially principle under Article 5(1)(f) of the UK GDPR provides that robust organisational and technical measures are in place to ensure the integrity of such data both when being transmitted by SMS and/or email, and when being held/accessed on the online platform. The ICO has produced guidance on security[7] that may be of use in considering the security measures to implement.

When opting in or out, it is important to distinguish between an individual giving their permission to receive notifications online, and relying on the Article 6(1)(a) lawful basis of consent for processing that person's data online. Indeed, consent is only appropriate if the controller can offer data subjects real choice and control over how their data is used, as opposed to giving them control over which communication method they wish to receive. The paying parent would likely be obligated to receive letters (and provide data to CMS where appropriate), whether online or otherwise, notifying them, for example, of the action they must take with regards to their child maintenance case and highlighting potential enforcement action. As such, due to the lack of genuine choice or control over how their data is used, consent would likely not be an appropriate basis in this instance.

Considerations regarding the accuracy of the data being stored, accessed and transmitted on the digital platform must be taken into account. In particular, regard needs to be given to the accuracy of data used to digitally verify individuals. In accordance with the accuracy principle, steps must be taken to ensure this data is kept up to date and accurate. Further steps need to also be taken to correct or erase any inaccurate personal data on the online platform. The ICO has produced guidance on the right to erasure[8] and rectification[9].

Controllership and data processing arrangements between organisations

It is unclear what the relationship is between DWP and HMRC in relation to the use of unearned income data and other categories of data potentially being shared to enable DWP to calculate liabilities. DWP and HMRC need to clearly establish their relationship and ensure clarity of controller, joint controller and

[7] Security | ICO
[8] Right to erasure | ICO
[9] Right to rectification | ICO

processor roles and responsibilities where necessary as required by Articles 24-29 of the UK GDPR. The ICO has produced guidance on this which may assist[10].

If this is a controller-processor arrangement, both parties must put a written contract in place which meets the minimum standards set out in Article 28 of the UK GDPR[11], or update existing contracts to take account of the new arrangement regarding unearned income data.

If DWP and HMRC are joint controllers for such processing, a transparent arrangement must be put in place, as required by Article 26 of the UK GDPR. In this context, it is good practice to put a data sharing agreement (DSA) in place, as recommended in the ICO's Data Sharing Code of Practice[12]. In particular, any DSA should clearly outline what each party should do in the event of an individual rights request under the UK GDPR.

The above considerations may be equally applicable between DWP and other bodies, such as the organisations that will be mandated to share data upon DWP's request. Such organisations are obligated to comply with information requests under regulation 4 of the Child Support Information Regulations 2008. As such, these organisations will likely be relying on the Article 6(1)(c) lawful basis of legal obligation to share such data. This would have implications for individual's data rights, in particular the right to object, regarding the disclosure of their data from these organisations to DWP. DWP should take such implications into account when establishing its relationship with these organisations.

The ICO is happy to provide further input on these matters and welcomes further engagement from DWP on these proposals. We look forward to receiving an A36(4) consultation on changes to the legislation.

Information Commissioner's Office

August 2021

[10] Controllers and processors | ICO
[11] Contracts | ICO
[12] Data Sharing: a code of practice | ICO