Information Commissioner's Office

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 of Work and Pensions' consultation on the draft Pensions Dashboards Regulations 2022

About the ICO

The Information Commissioner (ICO) has responsibility for promoting and enforcing data protection and information rights. This includes responsibilities under 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). The ICO is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO provides guidance and support to individuals and organisations, aimed at helping organisations to comply, and it takes appropriate action when needed.

Introduction

The ICO welcomes the opportunity to reply to the Department of Work and Pensions' (DWP) consultation on the draft Pensions Dashboard Regulations 2022 (Regulations). The ICO support the use of personal data to modernise the pensions industry in a manner that will enable consumers to access their pensions data online, securely, and in a single location, allowing individuals to better plan for their retirement. We also support the high degree of control these Regulations aim to give consumers over their own data, provided the processing described in the consultation is carried out in compliance with data protection legislation which will enhance public trust and confidence in how their data is being used.

The ICO recognises the references made throughout this consultation that emphasise the importance of data protection compliance, including a dedicated section on UK data protection legislation in chapter 3. We also acknowledge our previous engagement with DWP and the Money and Pensions Service (MaPS) throughout 2021 regarding the Pensions Dashboard Programme (PDP).

The consultation also makes several references to the role of the ICO, particularly in the context of investigating breaches of data protection law and taking action. Whilst the ICO does indeed enforce compliance with data protection legislation, we would like to emphasise that we are an independent,

proportionate regulator that understands the potential impacts of different regulatory approaches, including economic impacts, and will consider these before deciding on a course of action.

This response will focus on areas that fall within the ICO's remit, including the processing of personal data through the central digital architecture and from data providers to dashboards. For the avoidance of doubt, though this consultation makes no reference to the term 'data provider', this response will use it when collectively referring to pension providers, schemes, trusts, DWP (in the context of providing state pension data to dashboards), third party administrators and integrated service providers, as is consistent with how the term is used on the PDP website[1].

Whatever form the future Regulations take, we recognise data sharing will be required to provide consumers with quick and easy access to their pension information. We wish to emphasise that data protection is not a barrier to this but provides a framework through which the different entities can share data in a fair, secure and proportionate manner.

Summary

This section provides a brief summary of the key points we have raised. More detail is provided in the main section of this consultation response.

It is important that controllership is established at each stage, along with the lawful basis that each of the relevant entities will be relying on, before any processing has commenced. Where consent is being relied upon, the individual must be given genuine choice and control over how their personal data is processed. To meet transparency obligations, such details along with other meaningful privacy information must be made clear to the individual prior to processing, particularly where legal obligation is being relied upon as this will have data right implications.

A data protection by design and default approach should be taken when developing the programme. This includes components of the central digital architecture, and in particular the ID service, to ensure protection principles such as data minimisation and storage limitation are effectively employed. This

[1] UK Pensions Dashboards Programme | Homepage

approach will also enable appropriate safeguards to be implemented into the processing so that UK GDPR requirements are met and individual rights are protected. Where appropriate, different entities involved should consider if they need to carry out a Data Protection Impact Assessment (DPIA), which are a vital part of the data protection by design approach and will help identify and reduce data protection risks.

The data processed, such as the find/view data and pension identifier tokens, must be adequate, relevant and limited to what is necessary and must not be held for longer than is needed in relation to the purpose. The data must be processed in a secure manner and remain accurate and up to date.

Data Protection Impact Assessments (DPIAs)

When developing aspects of the central digital architecture and individual dashboards, it is important that the relevant controllers adopt a data protection by design and default approach[2] to ensure they can 'bake in' data protection from the design stage throughout the life cycle of the processing activities. When designing the online platforms, controllers may wish to consider how digitisation could better facilitate individuals in exercising their data rights as well as how to accommodate individuals who may be less computer-literate.

DPIAs[3] are an integral part of data protection by design and default as they can be used to help controllers ensure they are processing personal data in a manner that is compliant with data protection legislation. Article 35 of the UK GDPR requires controllers to carry out a DPIA where processing is likely to result in high risk to individuals.

Annex C of the consultation clarifies that both DWP and MaPS are undertaking DPIAs. If high risk to individuals is identified through either or both DPIAs which cannot be sufficiently mitigated, the relevant controller(s) must formally consult with the ICO under Article 36(1) of the UK GDPR prior to carrying out the high risk element of the processing. In such instances the ICO will provide written advice within 8 weeks, or 14 weeks in complex cases. As the Regulations relate to the processing of personal data, it would also be expected that DWP consult with the ICO during the preparation of these Regulations under Article 36(4) of the UK GDPR, though as noted earlier we recognise the prior engagement that

[2] Data protection by design and default | ICO
[3] Data protection impact assessments | ICO

has already taken place between DWP, MaPS and ICO. DCMS have produced guidance on the application of Article 36(4)[4].

Annex C also confirms DWP and MaPS intend to publish elements of their DPIAs when the Regulations are laid before parliament. Though not a requirement under UK GDPR, the ICO supports decisions to publish DPIAs or segments of DPIAs, where appropriate. Organisations should actively consider the benefits of doing so as in addition to demonstrating compliance, publication can engender public trust and confidence.

Other relevant entities may wish to consider carrying out a DPIA prior to commencing processing described in the consultation. The ICO has published a list of operations that require a DPIA under Article 35(4), some of which require a DPIA automatically and others only when they occur in combination with one of the other items.

Under Article 35(4), the matching, combining or comparing of data from multiple sources is one of the operations that automatically requires a DPIA. Chapter 3, sections 21-39 explains that when receiving find data, data providers will be obligated to conduct a data matching exercise with their internal records to identify if individuals hold pensions with them. From the description in the consultation, this may fall within scope of the aforementioned processing operation under Article 35(4), meaning data providers may need to undertake a DPIA before such processing is carried out.

From our previous engagement with MaPS and DWP, the ICO understands that currently, and subject to limited exemptions, pension providers are already required to match members who request their pension value information and send the information to that individual. As such, data providers may already possess a DPIA covering their particular matching process, which may need to be updated to take account of the likely increase in the scale of data matching that will be conducted when connecting to the digital architecture and responding to find requests. DPIAs are iterative documents which need to be kept under review and updated following substantial change to the nature, scope, context or purpose of processing.

Use of consent

[4] Guidance on the application of Article 36(4) of the General Data Protection Regulation (GDPR)

Chapter 3 of the consultation explains that once an individual consents, MaPS issues a find request of the individual's asserted and self-asserted data via the Pension Finder Service (PFS). The consultation does not seem to specify the exact UK GDPR Article 6 lawful basis under which data is processed within the digital architecture for the purpose of sending out a find request. However, it is clear that the individual must provide consent via the Consent and Authorisation Service (C&AS) to have their data sent out by MaPS.

It is important here to make a distinction between individuals providing their permission to MaPS for their find data to be processed though the digital architecture and relying on the Article 6(1)(a) lawful basis of consent under which to process the data. We cannot overstate the importance of establishing the correct lawful basis prior to processing as it can be difficult to change after processing has commenced. In particular, you cannot usually swap from consent to another basis.

It is only appropriate to rely on consent where the individual is given genuine choice and control over how their data is used, in other words, that it is freely given. As discussed during our previous engagement, and highlighted in Recital 43 of the UK GDPR, there may be a perceived imbalance of power between individuals and public authorities such as MaPS, which might make it difficult to demonstrate any consent given was done so freely. As such, the ICO generally advises public authorities to avoid reliance on consent as a lawful basis, unless the authority is confident the consent was freely given and can clearly document their decision making to justify why it is the most appropriate basis, in accordance with their accountability obligations.

On the assumption Article 6(1)(a) is being relied upon, the UK GDPR sets a high standard for consent which must be as easy to withdraw as it was for the individual to provide, as detailed in our guidance[5]. This standard would also apply to individuals giving consent for delegated access to third parties such as financial advisors. The ICO recognises that such considerations have been referenced throughout the consultation and we acknowledge the degree of control these the proposals aim to give individuals over the use of their personal data.

[5] Consent | ICO

Transparency, lawful basis and individual rights

Transparency is a legal requirement under Article 5(1)(a) of the UK GDPR and a key component of fairness. Prior to processing, clear and comprehensive information on how personal data will be processed, known as privacy information, must be provided to individuals in order to meet transparency obligations. Chapter 1, section 20 confirms that individuals will be provided with privacy information about the collection and use of their data. It is often effective to provide privacy information using a combination of different techniques including layering and just-in-time notices.

Given the various data flows and the different entities involved it is important that individuals are given meaningful privacy information about which controllers are processing their data at what stage and under what lawful basis. The latter point is of particular importance as individual's rights will vary in applicability depending on which lawful basis is relied upon. We would also want to avoid individuals believing they could revoke consent where the processing of concern is being carried out under a different lawful basis.

It is also important to make clear to individuals what processing will take place within the central digital architecture, and hence may likely be under the lawful basis of consent, and what processing will be outside of the architecture, such as data matching and returning of view data from the data provider to the dashboard. This may not be immediately obvious to users making requests through the dashboards who would likely view the process as a single system and may misdirect their individual rights requests. For example, if a dashboard user makes a request for erasure to MaPS, the user should be aware that whilst this may erase data held with the central digital architecture (such as pension identifier tokens in the C&AS), this would not erase data held outside of the architecture such as the find data sent to data providers, and that a separate request would need to be sent to the relevant pension scheme.

Similarly, individuals should be made aware that any additional information they provide to data providers following a 'possible match' will also be processed outside of the central digital architecture. This will allow individuals to make their own informed, risk-based decision on whether to proceed. This could also be made clear in the error message described in chapter 3, section 33 of the consultation.

Given that data providers will be legally obligated to connect to the digital architecture and provide view data upon request, it seems likely that they will be relying on the legal obligation lawful basis under which to process such data. Indeed, chapter 3 explicitly states that pensions schemes may rely on legal obligation as their lawful basis for returning view data to dashboards. This will have data right implications and so it is important meaningful privacy information is provided to individuals so they have reasonable expectations when exercising their rights.

The requirement to provide privacy information is also a right under Articles 13 and 14 of the UK GDPR, known as the right to be informed. In addition to the privacy information that will be provided to individuals as noted in chapter 1, section 20, data providers may need to update their existing privacy information to take account of any new processing activity that results from the Regulations. Dashboard providers will also need to make available the necessary privacy information. The ICO has produced guidance on the right to be informed, including a list of the categories of privacy information controllers must provide[6].

Controllership and data processing arrangements

The consultation describes multiple entities interacting with one another, processing data at various stages including MaPS, DWP, pension schemes, dashboard providers and the suppliers of the PFS and C&AS. These bodies must clearly establish their relationship with one another to ensure clarity of controller, joint controller and processor roles in accordance with Articles 24-29 of the UK GDPR.

Chapter 3, section 6 clearly establishes the view that MaPS, DWP, pension schemes and dashboard providers are separate controllers who successively process data in a chain of operations with one another. It is not for the ICO designate or sign off controllership of specific entities. However, when establishing controllership, whether separate or joint, several factors should be taken into account including the degree of independence they exercise and what role they play in determining the means and purpose of processing. The ICO outlines this and more in our guidance[7] and detailed guidance[8]. The ICO recognises the reference to such guidance in chapter 3, section 9.

[6] Right to be informed | ICO
[7] Controllers and processors | ICO
[8] Controllers and processors | ICO

When sharing data as separate controllers it is good practice, where appropriate and practical, to enter into a data sharing agreement (DSA) with other controllers involved, as recommended by the ICO's Data Sharing Code of Practice[9]. Any DSA needs to clearly outline the roles and responsibilities of each entity, such as setting out what each party should do when an individual rights request is received.

Chapter 3, section 11 illustrates the different data flows and controllership of each entity, however, it does not appear to address controllership of the ID service supplier. We recognise that the separate supplier for the ID service is yet to be sourced. Chapter 3, section 28 notes that MaPS will process the verified data elements from the ID service, but the relationship between MaPS and the ID service supplier is not as clear. Are they also independent controllers successively processing data in a chain of operations between one another, or could they be considered joint controllers?

If it is established that MaPS and the ID service supplier are joint controllers for the data processed by the ID service and/or the subsequent processing of verified data elements by MaPS, then a transparent arrangement must be put in place as required by Article 26 of the UK GDPR. DSAs can also be used to help joint controllers put such arrangements in place. If this is a controller-processor arrangement, both entities need to put in place a written contract that meets the minimum standards detailed within Article 28 of the UK GDPR.

Annex B, section 4 explains that Capgemini in partnership with Origo will deliver the PFS, C&AS and the Governance Register components of the central digital architecture, which appear to be vital elements needed to enable find requests to be sent out. The consultation does not seem to specify its relationship with MaPS who the consultation establishes is the controller for issuing find requests. Assuming the PFS and C&AS supplier will be processors, DWP may wish to clarify if they will both be independent processors, or if Origo will be a sub-processor of Capgemini. If so, there are additional contractual requirements[10] and Capgemini must only engage with its sub-processor with the controller's prior authorisation and under a written contract.

Data minimisation

[9] Data sharing: a code of practice | ICO
[10] Contracts | ICO

In accordance with the data minimisation principle under Article 5(1)(c) of the UK GDPR, any personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Controllers should consider the different aspects of the programme where this applies. For example, the asserted identity data that the user is required to provide to the ID service must be limited to what is necessary to verify the individual. Also, minimum data must only be collected through the digital architecture for the purpose of the find and view functions.

Data minimisation must also be considered for processing outside of the central digital architecture. For example, data providers must only process the find data that is necessary to identify pension records via their data matching exercises. The ICO recognises that the flexibility built into the Regulations provide data providers with the discretion to decide which elements of the find data they receive are necessary to identify their own matches, as noted in chapter 2, section 9. Data providers must consider data minimisation when setting their own matching criteria.

As data providers have discretion over which elements of the find data they match, it may be wise, if possible, to consider if this can be monitored during the test phase described in chapter 5, section 8, to see if certain data elements are consistently unused by data providers for matching, indicating they are not necessary for that purpose. This could then be used the refine and narrow the data elements required to find matches, without sending excess find data to schemes via the PFS.

Find data is made up of asserted information verified by the ID service and self-asserted information. From our understanding the users are required to input the asserted information. The glossary notes that users can elect to provide the scheme with the additional self-asserted information. If all the self-asserted data is optional this would appear to align with the spirit of the data minimisation principle. However, the principle also requires that data being processed is 'adequate' meaning the controller must be satisfied that the find data they process is sufficient to fulfil the stated purpose (ie to accurately identify matches). For instance, chapter 3, section 23 includes national insurance numbers (NINo) as self-asserted data. Would a data provider reasonably be able to find a match if the user elects not to provide their NINo? These two aspects of data minimisation should be carefully balanced to ensure processing is fair and proportionate.

The above data minimisation considerations are equally applicable to other aspects of the consultation, for example, the survey data collected by MaPS from data providers must be adequate, relevant and limited to what is necessary to assist in the evaluation of the dashboard service, as described in chapter 7.

Data retention

Personal data stored both within and outside of the central digital architecture 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 needed runs the risk that it will be become inaccurate, irrelevant, excessive or otherwise out of date.

It is important that any existing appropriate retention polices from the various entities involved are updated to take account of the any new categories of personal data that will be processed as a result of these Regulations, and that such polices are reviewed at regular intervals. For example, data provider retention periods should be updated to ensure the find data they receive following a request is held for no longer than is necessary in relation to the processing purpose.

We understand from the consultation and our prior engagement that find and view data will not be stored within the central digital architecture itself. However, it appears that pension identifier (PeIs) tokens will be stored within the C&AS component of the digital architecture. It is not clear from the consultation if PeIs are considered personal data. The description of PeIs in Annex B explains they do not contain any information about the individual. However, the view data description in chapter 3 notes that schemes process PeIs as independent controllers, which would imply they are considered personal data. Though PeIs may not directly identify individuals, you should consider if they can indirectly identify individuals in combination with other information. The ICO has produced guidance covering what constitutes personal data[11].

Assuming PeIs are considered personal data, the identifier tokens should not be held within the digital architecture for longer than is necessary. As such,

[11] What is personal data? | ICO

consideration needs to be given to registered PeIs that have not be used for a significant amount of time to enable dashboards to retrieve pensions information. Similarly, dashboard providers must consider PeIs registered on their individual dashboards following an individual's consent to do so. Consent does not last forever and is likely to degrade over time. We recognise that such retention limits will be determined by MaPS standards as noted in chapter 7, section 17.

It is important to recognise that personal data held for too long will, by definition, be unnecessary. Most Article 6 lawful bases require the processing to be necessary for the specific purpose, meaning there is unlikely to be a valid lawful basis under which to process unnecessary data, including storing it. To reduce this risk, data should be erased or anonymised when it is no longer needed.

The ID service and accuracy

This response has referred to the ID service several times as it is a key component of the central digital architecture with significant data protection implications. We understand that whilst Capgemini and Origo have been contracted as the suppliers of the three other components of the architecture, a separate supplier will be sourced for the ID service. Annex B, section 5 references the DCMS UK digital identity and attributes trust framework, noting for now that an interim provider will be appointed until the trust framework is in place.

When precuring a digital identity supplier, it is important to consider the data protection and wider privacy implications of whichever supplier is chosen. In particular, a data protection by design approach should be taken to the process, including carrying out a DPIA to ensure that any risks in the processing of personal data for implementing the ID service are appropriately mitigated against and sufficient safeguards are put in place. The ICO has published a digital identity position paper[12] to help organisations understand our position on digital ID.

The ICO echo DWP's call in chapter 5, section 55 that it is vital schemes are doing what they can to improve the accuracy of the data which will be integral to the success of pension dashboards. The accuracy principle under Article 5(1)(d)

[12] ICO Digital Identity Position Paper

of the UK GDPR requires that organisations ensure data remains accurate and up to date.

Regard needs to be given to the accuracy of the data that will be used to digitally verify users and corroborate the asserted identity attributes individuals provide to the ID service. Inaccurate or out of date data could lead to verification issues resulting in members being unable to access their data and being unfairly refused dashboard services despite providing accurate asserted identity attributes on their end.

The accuracy principle is equally applicable to other aspects of the PDP and should be considered throughout. For example, the Regulations propose the requirement to provide individuals with a projection of what their pension might be worth in retirement. It is important that these projections are based on accurate data as they may influence an individual's behaviour. Inaccurate data may mean individuals are unable to take the right action when planning for retirement, potentially leading to financial hardship. As such, it is vital that steps are taken to rectify or remove any inaccurate data without delay.

Automated processing

The consultation refers to small aspects of the pension dashboard process being automated and highlights the need for schemes to eventually shift towards automation to enable instantaneous responses. The consultation encourages pension schemes to think ambitiously about how they can put mechanisms in place to facilitate this.

It is unclear if this, or other aspects of the project that involve such processing would constitute solely automated processing as defined in Article 22 of the UK GDPR. If any processing described within the consultation, or planned in the future, falls within scope of this definition, it is important to remember that individuals have the right not to be subject to solely automated processing, which results in a legal or similarly significant effect concerning the individual. Such processing can only proceed where an exception in Article 22(2) applies. Privacy information must also include details of the existence of automated decision-making, including profiling. The ICO has produced detailed guidance on the data protection requirements when using solely automated processing[13]

[13] Automated decision-making and profiling | ICO

Particular consideration should be given to any potential risks that may arise to individuals if the ID service supplier relies on solely automated decision making to verify individuals.

Security

The Regulations propose a novel and ambitious initiative which will lead to new data shares between multiple entities concerning a significant number of individuals. As such, it is paramount that sufficient security measures are put in place to protect individual's data when being transmitted through the central digital architecture and from data providers to dashboards.

The ICO recognises that the governance register is being developed as part of the digital architecture to oversee the dashboard ecosystem and provide assurances that it is kept safe and the required security standards are met. These standards must comply with the integrity and confidentially principle under Article 5(1)(f) of the UK GDPR which provides that robust organisational and technical measures are in place to ensure the integrity of the data.

The pensions data that will be processed is of a particularly sensitive nature, and a breach of such data, or an error resulting in view data being inappropriately disclosed to the wrong person, could potentially lead to significant detriment or worry for the individuals involved.

Chapter 5, sections 5-6 detail the number of pension schemes and memberships throughout Great Britain. As such, the volume of personal data that will be processed as a result of these Regulations will be very high. This coupled with the requirement to undertake matching exercises and provide view data on demand, and the option to export data from dashboards as described in chapter 7, section 26-36, means that great care must be taken to ensure personal data is held and processed securely.

Considerations that organisations must take are detailed in Article 32(1) of the UK GDPR, which include the cost of implementation and the risk of severity for the rights and freedoms of the individual. The level of security that is implemented should align to the level of risk and should be documented in the

DPIA(s). The ICO has produced guidance on security[14] which may be of use when considering the security measures to implement.

The ICO is happy to continue engaging with DWP and MaPS on the PDP, and to clarify any points raised above.

11 March 2022

[14] Security | ICO