The Information Commissioner’s response to Cabinet Office’s public consultation: *The UK Single Trade Window: Consultation on features to inform design and legislation*

About the ICO

1. The 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 Network and Information Systems Regulations 2018 (NIS), 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.
2. The Information Commissioner’s Office (ICO) welcomes the opportunity to respond to the Cabinet Office’s public consultation: *The UK Single Trade Window: consultation on features to inform design and legislation* (the consultation).

Summary

1. We recognise the importance of driving efficiencies in the operation of trade across the UK border, by avoiding the need for duplication of information across a range of different portals. We also recognise that the development of a Single Trade Window (STW) is an important opportunity to coordinate the better use of data across government, collecting data relating to cross border trade through a single platform and then sharing further within government.
2. Public trust and confidence are important factors in successful public sector initiatives involving personal data. Developing a framework for the STW that integrates high standards for privacy and a positive approach to data protection when handling personal data is more likely to secure and maintain that trust. A data protection by design and default approach to the STW will help Cabinet Office and HMRC in achieving these aims, and should include

* undertaking a data protection impact assessment (DPIA)
* assessing the necessity and proportionality of the processing and sharing of personal data
* undertaking a comprehensive mapping exercise of the data flows involved in the STW
* establishing the necessity and proportionality of the processing, including building on the fundamental principles of data protection
* ensuring the STW is fair and transparent, and supports individual rights, and
* ensuring that appropriate protections are in place for any international transfers of personal data.

Background

1. The consultation explores the development of a STW to create a single gateway for all transactional data from traders into government in relation to trade across the UK border. It focuses on the collection, use and sharing of data within government; government’s sight and use of supply chain data; and the need for international data sharing.
2. The data within scope of the proposals relating to the STW is likely to include a significant volume of information that does not relate to individuals, but it will include personal data. Our comments are limited to issues relating to personal data and not to other issues outside our remit.
3. Decisions that HMRC and Cabinet Office make about how to deliver the STW will affect the data protection issues that arise and the potential for risk. We have therefore confined most of our comments at this time to overarching principles. We will welcome further engagement with Cabinet Office or HMRC to discuss specific data protection issues in more detail, once they have reached a settled position about how the STW might operate.

Data protection by design and default

1. Ensuring that HMRC collects and then shares data responsibly in the context of the STW will be an important element in supporting public trust and confidence, in addition to the efficiencies and other benefits to business and the wider economy that the STW is expected to deliver. Adopting a data protection by design and default approach[[1]](#footnote-1) will be essential as the STW will involve new data sharing initiatives and organisations might use personal data for new purposes. Keeping this approach in focus will ensure that Cabinet Office and HMRC develop the STW in a privacy enhancing way. This will not only help ensure compliance with the fundamental principles and requirements of data protection legislation, but will also assist government and the other organisations involved in demonstrating their accountability for their processing of personal data.

*Data protection impact assessment*

1. A data protection impact assessment (DPIA) is a useful tool to help organisations identify risk and assess potential mitigating steps. Undertaking a DPIA at an early stage will support a data protection by design approach to the STW and will help identify areas of risk which can inform future decisions on the project as they arise. It is also important to note that a DPIA is mandatory if the processing is likely to result in a high risk to individuals, or meets specified criteria[[2]](#footnote-2). The DPIA will need regular review as the project develops.

*Data mapping and data sharing*

1. Efficient sharing of data in the public sector can improve insights and outcomes, and increase options for recipients. Data protection law provides a framework to enable processing of personal data to be fair, lawful and transparent.
2. Data sharing is an important aspect of the STW that HMRC will operate. This is to be a new platform between border authorities and agencies and government, for both import and export purposes. Aims behind this proposal include avoiding the need for traders and intermediaries to use multiple portals and avoiding duplication. HMRC will share data it receives with other government departments and public bodies.
3. This approach might result in a reduction in the amount of personal data that government needs to process in some respects, as well as helping to address other inefficiencies. However, it will also introduce new systems for the collection of the data and there could be considerably more sharing of data between a larger number of participants. This will apply to commercial organisations inputting data into the STW and to HMRC’s data sharing with government departments and public bodies.
4. For example, commercial organisations may benefit from the joint approach of making submissions to the STW by ‘multi-filing’, which might help to streamline the process. Government will decide on how best to manage the legal responsibility for filing in these situations. However, multi-filing will need a collaborative approach to the protection of the personal data involved. Similarly, HMRC will need to collaborate closely with those organisations with whom it will share personal data.
5. The potential for complex data sharing relationships between commercial organisations and the public sector in the STW suggests the need for a comprehensive data mapping exercise to plot out the proposed data flows, as part of a data protection by design approach. Such an exercise needs to include clarity about the specific fields of personal data that HMRC or others might require for each of the stated purposes. This will clarify specific areas of challenge and opportunity. More specifically, a mapping exercise is likely to highlight interdependencies and complexities that HMRC or Cabinet Office will need to address, including areas which might present risks to individuals. It is also likely to highlight where HMRC or wider government might usefully play a part, for example, by signposting guidance to help organisations comply with their obligations under data protection legislation.
6. Any data mapping exercise will feed into the DPIA and will form part of the overall assessment it contains. It should also be kept under review and reflect any changes as the project develops.
7. Before data sharing takes place, Cabinet Office and HMRC will also need to ensure that they have established a clear framework for data sharing with all organisations concerned. Data sharing agreements set out the purpose of data sharing, including what happens to the data at each stage. They also help everyone participating in the data sharing to be clear about their roles and responsibilities. Public authorities involved in the STW will also need to include details of the types of information they include in their freedom of information publication schemes. The ICO’s data sharing information hub, which includes the ICO’s data sharing code, provides valuable resources[[3]](#footnote-3) in this context.
8. If organisations, including HMRC, do not need personal data to achieve their objectives, then they should seek to use anonymous information instead. We have published a call for views on our draft guidance on anonymisation which is likely to be of assistance[[4]](#footnote-4) in this respect.

*Necessity and proportionality*

1. Most of the potential lawful bases for processing under UK GDPR require the processing to be necessary[[5]](#footnote-5). Necessity in this context is closely linked to the need for proportionality, and together, these principles help to establish that the processing is fair and results in fair outcomes. Controllers need to be satisfied that the processing is a targeted and proportionate way to achieve the aim and that the aim cannot be achieved in a less intrusive way.
2. The principles of necessity and proportionality are closely linked to the fundamental data protection principles of principles of purpose limitation,[[6]](#footnote-6) data minimisation[[7]](#footnote-7) and accuracy[[8]](#footnote-8). The processing will also need to comply with the other data protection principles, including requirements for transparency and security[[9]](#footnote-9). As part of a data protection by default approach, Cabinet Office and HMRC will therefore need to ensure, for example, that in the context of the STW it will only process the personal data that is necessary to achieve its specific purposes and that the personal data it collects and shares is adequate for those purposes. Giving consideration to such matters will assist in identifying areas of potential risk, or opportunities for pursuing more privacy-focused options.
3. Cabinet Office and HMRC will also need to scope out how these data protection principles will apply in each instance of processing and data sharing in the design of the STW to ensure that they build in the necessary protections for personal data. For example, they will need to cross reference the purposes for which each government department or public body will properly require data from the STW. In this situation, depending on the purpose involved, it may be that some public bodies require more or less personal data than others. Processes should set out how HMRC will ensure that the personal data traders have to provide in the STW does not exceed what is required and that HMRC does not go on to share more than a public body actually requires.
4. Specifically, the consultation invites views on whether the STW should enable a voluntary approach to the provision of supply chain data. It is unclear whether this information will, in fact, include personal data and Cabinet Office and HMRC will need to scope this out. Assuming that this might be the case, they will also need to evaluate whether the processing of such personal data is necessary and proportionate. In particular, they will need to consider if this personal data is necessary when it is not required from all participants and is voluntary in nature.

*Transparency and fairness*

1. Making clear at the outset why HMRC and other organisations will collect personal data and how and why they will share it are, as mentioned above, vital elements of a data protection by design and default approach. Being clear, open and honest about the processing is also likely to promote public trust and confidence. Taking this approach will therefore help to ensure that the processing is fair and transparent. This approach also means that data protection issues can be addressed and factored into the STW design process at the earliest possible stage.
2. The journey of an individual’s personal data through the STW and then on to other public bodies may be complex. This might give rise to particular challenges around the potential for ‘invisible processing’ particularly where organisations do not collect the personal data directly from the individual. Cabinet Office and HMRC will need to consider how they can provide meaningful privacy information to individuals in ways that will be clear and understandable.
3. In the same vein, Cabinet Office and HMRC will also need to provide clear frameworks as part of the STW so that the organisations involved can support individuals’ rights and individuals will know how to exercise them.
4. All transparency measures will need regular review to ensure that they are fit for purpose as the policy develops.

*International transfers*

1. The consultation proposes that in due course, the STW system can operate alongside similar systems in other countries and territories and that government will exchange data between those systems. Government will need to consider the legal gateways it will need to facilitate this, as well as satisfying itself of the necessity and proportionality of any such data sharing in relation to any personal data that may be involved.
2. Government will be aware that UK GDPR restricts the transfer of personal data to countries outside the UK or to international organisations (restricted transfer), unless there are ‘adequacy regulations’, appropriate safeguards, or the restricted transfer is covered by an exception under article 49 UK GDPR. Government will therefore need to consider how it can make compliant restricted transfers to other countries in relation to the STW. It will also need to ensure that individuals receive information about the existence of any proposed international transfers so that they understand the circumstances in which government might share their personal data to other countries or territories.

Consultation

* 1. We welcome the opportunity for further engagement with Cabinet Office and HMRC on these proposals at an early stage as they develop. In addition, we look forward to receiving requests for formal consultation under article 36(4) UK GDPR in relation to any proposed legislative measures involving processing.

1. Article 25 UK GDPR [↑](#footnote-ref-1)
2. [Data protection impact assessments | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) [↑](#footnote-ref-2)
3. [Data sharing information hub | ICO](https://ico.org.uk/for-organisations/data-sharing-information-hub/) [↑](#footnote-ref-3)
4. [ICO call for views: Anonymisation, pseudonymisation and privacy enhancing technologies guidance | ICO](https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-anonymisation-pseudonymisation-and-privacy-enhancing-technologies-guidance/) [↑](#footnote-ref-4)
5. Article 6 UK GDPR [↑](#footnote-ref-5)
6. [Principle (b): Purpose limitation | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/) [↑](#footnote-ref-6)
7. [Principle (c): Data minimisation | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/) [↑](#footnote-ref-7)
8. [Principle (d): Accuracy | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/) [↑](#footnote-ref-8)
9. [Security | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/) [↑](#footnote-ref-9)