Cabinet Office

v2. 07/11/24 - with suggested changes from original that was drafted in July 2023
[requires COLA - yes, digital, final DPO sign off]

DATA SHARING AGREEMENT
("Memorandum of Understanding")

Between

THE CABINET OFFICE

And

Contracting Authorities participating in Public Procurement

Relating to

Find a Tender Service

---

1. **Memorandum of Understanding overview**

This memorandum of understanding ("MoU") is made between the Cabinet Office and the contracting authorities listed in Annex 3, referred to jointly in this document as "the Parties". It remains valid until superseded by a revised MoU mutually endorsed by the Parties.

A representative from each contracting authority will be asked to agree to the terms of this MoU at time of onboarding onto the online system referenced in the Procurement Act 2023 (Act) and named in the Procurement Regulations 2024 (regulations) as "the central digital platform" (available at https://www.find-tender.service.gov.uk/). This service is also known as Find a Tender Service (FTS)).

The Cabinet Office will take responsibility for publishing and maintaining the list of signatories for this MoU.

2. **MoU Purpose**

The purpose of this MoU is to explain the nature of the personal and sensitive data collected and shared on FTS.

3. **Overview of FTS**

The purpose of FTS is to facilitate the publication of procurement notices and related information as required by the Procurement Act 2023 and Procurement Regulations 2024.

It is also to facilitate participation in public procurement where contracting authorities require suppliers to register with the service provided by the Cabinet Office and complete the "Supplier Information" section. This supplier information can then be shared from the Cabinet Office digital system (FTS) by the supplier to the relevant contracting authority for process and review at the time of bidding. This is done via a digital API sharecode or a manual PDF file share.

The information collected on FTS contains both personal information and personal data relating to criminal convictions or offences of individuals. Further detail on the data collected can be found in the Privacy Notice**2024-06-07_Central Digital Platform privacy notice - DRAFT OFFSEN-2 (1).docx**

Commented [1]: insert link to privacy notice URL on FTS

4. **Cabinet Office and employing government department's responsibilities as joint data controllers**

Under Article 26 (Joint Data Controllers) Cabinet Office and the employing departments including their Arms Length Bodies (if being represented by their sponsoring departments on the Central Digital Platform) will act as joint data controllers, in respect of any personal data pursuant to this MoU. The parties agree that they are joint data controllers when a participating organisation uses the Central Digital Platform to tender. For this agreed purpose the Cabinet Office and each participating organisation are joint data controllers because they are processing the same personal data (the personal data used for the procurement) for the same purposes (complying with the Procurement Act 2023) and by the same means (using the Central Digital Platform).

Cabinet Office will only process personal data to the extent necessary for the shared purposes. This is to facilitate compliance with the Procurement Regulations 2024 by a contracting authority in whose procurement the supplier wishes to participate.

The parties will ensure that they have appropriate technical and organisational procedures in place to protect any personal data they are processing. This includes unauthorised or unlawful processing, and protection against any accidental disclosure, loss, destruction or damage. Cabinet Office will promptly inform employing departments, and vice versa, of any unauthorised or unlawful processing, accidental disclosure, loss, destruction or damage to any such personal data. Both parties will take reasonable steps to ensure the suitability of their staff having access to such personal data.

Neither the Cabinet Office nor participating organisations will transfer any personal data it is processing outside of the UK and the European Economic Area, unless appropriate legal safeguards are in place, such as an adequacy decision, or a UK International Data Transfer Agreement.

5. **Specific Cabinet Office responsibilities as joint data controllers:**

- Carrying out any required Data Protection Impact Assessment for the overall platform and service.
- provide the digital service to facilitate compliance with the Procurement Regulations 2024 by a contracting authority in whose procurement the supplier wishes to participate
- Following Cabinet Office Data Security Guidance to ensure that the necessary measures are taken to protect personal data.
- Ensuring approved staff are appropriately trained in how to use and look after personal data, and follow approved processes for data handling.
- Ensuring staff have appropriate security clearance to handle personal information held as part of the database.

- Comply with the data protection principles, and with all relevant data protection legislation.
- Maintaining and adhering to a privacy notice and data retention policy.
- Responding to data subject requests made to Cabinet Office in relation to the information submitted and stored in the Supplier Information service.
- Providing a data sharing agreement for sharing the information submitted and stored in FTS with any separate data controllers.
- Secure transfer of personal data both internally and externally from CO. Details can be found at Annex 1.
- Cabinet Office is responsible for reporting any reportable breach within Cabinet Office to their Data Protection Office and the ICO within 72 hours, in consultation with the employing departments Data Protection Officer.
- making the essence of this joint controller agreement available to data subjects via the Cabinet Office privacy notice.

6. **Specific contracting authority responsibilities as joint data controllers:**

- Receiving, processing and publishing relevant information from Find a Tender service to support compliance with Procurement Act 2024.
- Following their organisational Security Guidance to ensure that the necessary measures are taken to protect personal data.
- Carrying out any required Data Protection Impact Assessment for any processing of data downloaded or otherwise extracted from the platform onto buyer systems, and their own procurement related activities.
- Ensuring staff are appropriately trained in how to use and look after personal data, and follow approved processes for data handling.
- Ensuring staff have appropriate security clearance to handle personal information.
- Ensuring an appropriate level of technical and organisational security for the personal data, including restricting access to the database to approved staff only and ensuring staff follow approved processes for data handling.
- Comply with the data protection principles, and with all relevant data protection legislation.
- Ensuring that the information received from Supplier Information is used for their own commercial processing or assurance purposes, that any necessary Privacy Notices are provided to data subjects.
- Responding to data subject requests made to them in relation to the information submitted and stored in FTS, rectification or erasure and liaising as necessary with the Cabinet Office.
- Secure transfer of personal data both internally and externally from the department.
- Review and disposal of procurement and contractual records and the secure transfer of information given to the contracting authorities from the supplier to the National Archives, as a matter of public record, at the end of the seven year data retention period.
- Employing departments are responsible for reporting any reportable data breaches within the department to their Data Protection Officer and ICO within 72 hours, in consultation with the Cabinet Office.

7. **Data retention**

The Parties shall not retain or process Personal Data for longer than is necessary to carry out the agreed purposes of supporting compliant procurement as required by the Procurement Act 2024.

Notwithstanding, the Parties shall continue to retain Personal Data in accordance with any statutory or professional retention periods applicable in their respective organisations.

8. **Publishing this MoU**

The Cabinet Office will take responsibility for publishing this MoU.

9. **SIGNATURES**

The signatories agree that the procedures laid down in this Agreement provide an acceptable framework for the sharing of information between themselves, and that it is in a manner compliant with their statutory and professional responsibilities.

By signing this agreement, the signatories undertake to accept responsibility for implementation of the terms of this Agreement within their own organisations.

Signatories must also ensure that they comply with all relevant legislation.

Signed by:

Department Name	**Cabinet Office**
Signed on behalf of Department Business Unit	***[Will be Euan]***
Print Name (Block Capitals)	
Date	***[add date finalised]***

Department	
Authorised personnel name signing on behalf of department	
Print Name (Block Capitals)	

Commented [2]: Can this by "signed" digitally. e.g just complete it on the platform?

Commented [3R2]: from a DP perspective it needs to be agreed by the other organisation. How that is done is not specified. I think email agreement from a suitably senior person (DD?) is fine, so long as we keep that record. Are there any other things you need departments to agree when they are onboarded? If so this could be added?

Commented [4R2]: If it was built into the service with a online questionnaire and they agree to it, would that be ok? They can still chose who fills this in - up to each entity to agree it.

Date	

Annex 1

Data Items under Joint Controllership

The personal and sensitive data that FTS may collect and will transfer to CAs, once shared by suppliers to that CA at the time of bidding

- name of supplier or connected person
- email address of supplier or connected person
- address of supplier or connected person
- date of birth of supplier or connected person
- nationality of supplier or connected person
- The criminal convictions data we may collect on individuals connected to your organisation relate to the grounds set out in grounds set out in Schedules 6 and 7 of the Procurement Act 2023. Further detail on the data collected can be found in the Privacy Notice.

Annex 2

Contacts Relevant to this Data Sharing Agreement

The Data Protection Officers for the Parties to this agreement are:

Cabinet Office – Steve Jones Email: dpo@cabinetoffice.gov.uk

Recipient Department – see annex 3

The individuals that have arranged this agreement are:

Role/Department	Name	Email
Policy lead, Cabinet Office	Olivia Bush	Olivia.bush@cabinetoffice.gov.uk

The individuals responsible for the monitoring of this agreement are:

Commented [5]: unsure?

Commented [6R5]: I don't know either

Commented [7R5]: sorry Steve - this is a question for the digital team

Role/Department	Name	Email

Annex 3: list CAs and authorised personnel that have registered on the Central Digital Platform and agreed to the terms of this MoU

Commented [8]: This will be handled digitally

Department name	Authorised personnel name	Authorised personnel	Date signed

- **end -**

DATA SHARING AGREEMENT

Between

THE CABINET OFFICE

And

Contracting Authorities participating in Public Procurement

Relating to

Supplier Information Service, a component of the Central Digital Platform - part of the Procurement Act 2024

10. This MOU is made between the Cabinet Office and the contracting authorities listed in Annex 3, referred to jointing in this document as the Parties. It remains valid until superseded by a revised MOU mutually endorsed by the Parties.

11. Contracting authorities will be asked to agree to the terms of this MoU at time of onboarding onto the system and the Cabinet Office will take responsibility for publishing and maintaining the list of signatories for this MOU.

11.1. **MOU Purpose**

The purpose of this MOU is to explain the nature of the personal data collected and processed as part of Supplier Information, a component of the Central Digital Platform - as detailed in regulation 6 of the Procurement Act 2024, and the roles of the Parties, who are joint-controllers of this data.

11.2. **Overview**

Supplier Information is the service provided by the Cabinet Office to collect the information about suppliers that is required by Contracting Authorities ("buyers") for the purpose of participating in public procurement in the UK. The data is provided and updated by suppliers at the point of bidding on a procurement and shared through Supplier Information to Contracting Authorities. The information is collated and used by Contracting Authorities during the public procurement assessment process and, where the Supplier is successful, in some instances, is published on Find a Tender Service e.g. the awarded Supplier details are published in a notice on Find a Tender Service. The information is also collated by the Cabinet Office into an amalgamated cross government database of commercial policy interests.

The information collected through Supplier Information contains both personal information and personal data relating to criminal convictions or offences of individuals. Further detail on the data collected can be found in the Privacy Notice: 2024-06-07_Central Digital Platform privacy notice - DRAFT OFFSEN.docx

11.3. **Cabinet Office and employing government department's responsibilities as joint data controllers**

Commented [9]: I'm assuming I only need to look at the first version of this above.

Commented [10R9]: yes exactly - thanks

Under Article 26 (Joint Data Controllers) Cabinet Office and the employing departments including their Arms Length Bodies and/or third parties used by the departments for Due Diligence will act as joint data controllers, in respect of any personal data pursuant to this MOU. Cabinet Office will only process personal data to the extent necessary for Suppliers to create and manage Supplier Information, and for Contracting Authorities to manage access of Supplier Information with their e-senders. For Cabinet Office specifically these are:

- providing a service for suppliers participating in public procurements, where they can input commonly used information that will be used by contracting authorities during the procurement process. Some of this information is mandated through legislation (specifically regulations 6-12 in the Procurement Act 2024)
- to enable tracking and measurement of the implementation of initiatives of the Procurement Act 2024.
- to continue to build an understanding of the Suppliers who participate in public procurement and their Connected Persons

The parties will ensure that they have appropriate technical and organisational procedures in place to protect any personal data they are processing. This includes unauthorised or unlawful processing, and protection against any accidental disclosure, loss, destruction or damage. Cabinet Office will promptly inform employing departments, and vice versa, of any unauthorised or unlawful processing, accidental disclosure, loss, destruction or damage to any such personal data. Both parties will take reasonable steps to ensure the suitability of their staff having access to such personal data.

Neither the Cabinet Office nor participating organisations will transfer any personal data it is processing outside of the UK and the European Economic Area, unless appropriate legal safeguards are in place, such as Model Contract Clauses.

11.4. **Specific Cabinet Office responsibilities as joint data controllers:**

- Carrying out any required Data Protection Impact Assessment for the service for related Cabinet Office activities.
- Maintaining and managing the service to support public procurement as per Procurement Act 2024.
- Maintaining and compiling the amalgamated Supplier Information database from Supplier submissions on the service.
- Following Cabinet Office Data Security Guidance to ensure that the necessary measures are taken to protect personal data.
- Ensuring approved staff are appropriately trained in how to use and look after personal data, and follow approved processes for data handling.
- Ensuring staff have appropriate security clearance to handle personal information held as part of the database.
- Comply with the data protection principles, and with all relevant data protection legislation.
- Maintaining and adhering to a privacy notice and data retention policy.
- Responding to data subject requests in relation to the information submitted and stored in the Supplier Information service.
- Providing a data sharing agreement for sharing the information submitted and stored in the Supplier Information service with any separate data controllers.

- Secure transfer of personal data both internally and externally from CO. Details can be found at Annex 1.
- Cabinet Office is responsible for reporting any reportable breach within Cabinet Office to their Data Protection Office and the ICO within 72 hours, in consultation with the employing departments Data Protection Officer.

11.5. **Specific contracting authority responsibilities as joint data controllers:**

- Receiving, processing and publishing relevant information from Supplier Information on Find a Tender service to support compliance with Procurement Act 2024.
- Following their organisational Security Guidance to ensure that the necessary measures are taken to protect personal data.
- Ensuring staff are appropriately trained in how to use and look after personal data, and follow approved processes for data handling.
- Ensuring staff have appropriate security clearance to handle personal information.
- Ensuring an appropriate level of technical and organisational security for the personal data, including restricting access to the database to approved staff only and ensuring staff follow approved processes for data handling.
- Comply with the data protection principles, and with all relevant data protection legislation.
- Ensuring that the information received from Supplier Information is used for their own commercial processing or assurance purposes, that any necessary Privacy Notices are provided to data subjects.
- Responding to data subject requests in relation to the information submitted and stored in the Supplier Information service, rectification or erasure and liaising as necessary with the Cabinet Office.
- Secure transfer of personal data both internally and externally from the department.
- Review and disposal of procurement and contractual records and the secure transfer of information given to the contracting authorities from the supplier to the National Archives, as a matter of public record, at the end of the seven year data retention period.
- Employing departments are responsible for reporting any reportable data breaches within the department to their Data Protection Officer and ICO within 72 hours, in consultation with the Cabinet Office.

11.6. **Data retention**

The Parties shall not retain or process Personal Data for longer than is necessary to carry out the agreed purposes of supporting compliant procurement as required by the Procurement Act 2024.

Notwithstanding, the Parties shall continue to retain Personal Data in accordance with any statutory or professional retention periods applicable in their respective organisations.

11.7. **Publishing this MOU**

The Cabinet Office will take responsibility for publishing this MOU.

12. **Annex 3: list CAs that have registered on the Central Digital Platform and agreed to the T&Cs.**

SIGNATURES

The signatories agree that the procedures laid down in this Agreement provide an acceptable framework for the sharing of information between themselves, and that it is in a manner compliant with their statutory and professional responsibilities.

By signing this agreement, the signatories undertake to accept responsibility for implementation of the terms of this Agreement within their own organisations.

Signatories must also ensure that they comply with all relevant legislation.

Signed by:

Department Name	**Cabinet Office - (insert BU name)**
Signed on behalf of Department Business Unit	
Print Name (Block Capitals)	
Date	

Department	**?**
Signed on behalf of Department Business Unit	**?**
Print Name (Block Capitals)	**{Name}**
Date	**{Date}**

Annex 1

Data Items under Joint Controllership that are shared

The personal data that Central Digital Platform collects and will transfer to departments are:

excluded information on grounds of mandatory exclusion to a supplier if the supplier or a connected person has been convicted of an offence (as per schedule 6 of Bill)	• As set out in regulations (Procurement Act 2024) to collect core information of suppliers, increase transparency in public procurement, protect public procurement and government spending • to assess individual and organisations who are connected to an organisation • allow for a full and fair due diligence when awarding procurement contracts
email address	• as part of Supplier Information if a Connected Person has any related criminal convictions and events associated with them
address	• for buyers to review when conducting their due diligence • for buyers to enter within their notices
date of birth	• determine the date of birth of Connected Persons
name (first and last name)	• gain the name of Connected Persons

Annex 3

Contacts Relevant to this Data Sharing Agreement

The Data Protection Officers for the Parties to this agreement are:

Cabinet Office – Steve Jones Email: dpo@cabinetoffice.gov.uk

Recipient Department – Insert Full Name Email: XXXXX@doman.com

The individuals that have arranged this agreement are:

Role/Department	Name	Email

The individuals responsible for the monitoring of this agreement are:

Role/Department	Name	Email