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 the signatories section, 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 It remains valid until superseded by a revised MoU mutually endorsed by the Parties.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 and other and other relevant procurement regimes for example Public Contracts Regulations 2015.

It is also to facilitate participation in public procurement under the Procurement Act 2023 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 FTS Privacy Notice**.**

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 and other relevant procurement regimes by a contracting authority in whose procurement the supplier wishes to participate
- Process the data provided for reporting and analytical purposes cross-government.
- 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 Officer 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 2023 and other relevant procurement regimes.
- 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 2023.

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:

Organisation name	Cabinet Office
Signed on behalf of organisation	Euan Slack
Role in organisation	Deputy Director, Digital Services and National Security and Risk Unit. Government Commercial and Grants Directorate
Date	23/12/2024

Organisation name	
Signed on behalf of organisation	
Role in organisation	
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 the supplier relating 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 published on FTS.