Joint data controller Memorandum of Understanding (MOU) under Article 26 UK GDPR

Between

THE CABINET OFFICE

And

The Contracting Authority 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 Authority agreeing to the MoU on Find a Tender service (FTS), 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 It remains valid until superseded by a revised MoU mutually endorsed by the Parties.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 on the online system referenced in the Procurement Act 2023 (Act) and named in the Procurement Regulations 2024 (regulations) as "the Central Digital Platform" (CDP) (available at https://www.find-tender.service.gov.uk/). This service is also known as Find a Tender service (FTS).

2. MoU Purpose

The purpose of this MoU is to explain the nature of the personal data collected and shared by the Cabinet Office to the Contracting Authority, and by the Contracting Authority to the Cabinet Office, in both cases via FTS. The MoU defines the role and responsibilities of the Cabinet Office and the role and responsibilities of participating Contracting Authority.

3. Overview of the 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 relevant procurement regimes such as the Public Contracts Regulations 2015.

FTS also facilitates participation in public procurement under the Procurement Act 2023 and Procurement Regulations 2024 where Contracting Authorities require suppliers to register with the service provided by the Cabinet Office and complete the "Supplier Information" section of FTS. This information is then stored on FTS and can then be shared from FTS by the supplier to the relevant Contracting Authority for processing and review at the time of bidding. This is done via a digital API sharecode or a manual PDF file download that can then be uploaded on the Contracting Authority's service that is used for accepting bids.

The information collected on FTS contains personal data, and may include data relating to criminal convictions. Further detail on the data collected can be found in FTS Privacy Notice. The personal data that is subject to joint control is detailed in Annex 1.

The legal basis for processing this personal data is UK GDPR Article 6(1)(c), namely that processing is necessary to comply with a legal obligation placed on us as the data controller. In this case that is the obligation of a Minister of the Crown (the Cabinet Office) to provide an online platform (Find a Tender service) for the publication of information required by the Procurement Act 2023 and for the collection and facilitation of sharing supplier information as required by the Procurement Regulations 2024

4. **Definitions**

Unless otherwise stated, the words and expressions listed below shall have the following meanings:

- GDPR: the UK General Data Protection Regulation.
- DPA 2018: Data Protection Act 2018.
- Data Protection Legislation: (i) the UK GDPR as amended from time to time (ii) the DPA 2018 as amended from time to time (iii) all applicable Law about the processing of personal data and privacy as amended from time to time.
- Controller, Processor, Processing, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer, Data Protection Impact Assessment: take the meaning given in the UK GDPR or, in respect of processing of personal data for a law enforcement purpose to which Part 3 of the DPA 2018 applies, the meaning in that part if different.
- Data Protection Principles: means the principles set out in Article 5 of the UK GDPR.
- Data Subject Rights: means those rights set out in Chapter III of the UK GDPR.
- Subject Access Request: means the rights of data subjects set out in Article 15 of the UK GDPR.
- Personnel: means all directors, officers, employees, agents, consultants and contractors engaged in the Processing of Personal Data.
- DPO: Data Protection Officer.

5. **The Parties responsibilities as joint data controllers**

Under Article 26 of the GDPR, Cabinet Office including any relevant connected organisations (if representing the Cabinet Office on FTS) 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 at any point at which they are processing the personal data in Annex 1. For this agreed purpose the Cabinet Office and the contracting authority that has agreed to this joint control arrangement are joint data controllers because they are processing the same data (the personal data used for the procurement) for the same purposes (complying with the Procurement Act 2023 and Procurement Regulations 2024) and by the same means (using FTS).

The Cabinet Office will only process personal data to the extent necessary to facilitate compliance with the Procurement Act 2023 and Procurement Regulations 2024.

The Parties will ensure that they have appropriate technical and organisational procedures in place to protect any personal data they are processing. This includes protection from unauthorised or unlawful processing, and protection against any accidental disclosure, loss, destruction or damage. Cabinet Office will promptly inform the contracting authority of has agreed to this joint control arrangement, 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.

The Parties will not transfer any personal data it is processing outside of the UK, unless appropriate legal safeguards are in place, such as an adequacy decision, or a UK International Data Transfer Agreement.

6. **Specific Cabinet Office (including any relevant connected organisations to the Cabinet Office) responsibilities as joint data controllers:**

- Carrying out any required Data Protection Impact Assessment in relation to the platform as a whole and the provision of the FTS service.
- Following Cabinet Office Data 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 held as part of the database.
- 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.
- Complying 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 the Cabinet Office in relation to the information submitted and stored in FTS and are under joint control as per this agreement, as well as requests for rectification or erasure and liaising as necessary with the Parties to this agreement. This includes providing assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.
- Providing a data sharing agreement for sharing the information submitted and stored on FTS with any separate data controllers.
- Securely transferring personal data both internally and externally from the Cabinet Office.
- Reporting any reportable breach within Cabinet Office in respect of personal data which is within the joint control of the Parties to their Data Protection Officer and the ICO within 72 hours, in consultation with the joint controller Contracting Authority's Data Protection Officer (or equivalent).
- Taking responsibility for maintaining the list of signatories for this MoU and providing it to data subjects as requested.

7. **Specific Contracting Authority responsibilities as joint data controllers:**

- 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.
- 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 held as part of the database.
- 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.
- Complying 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 the Contracting Authority and are under joint control as per this agreement, as well as requests for rectification or erasure and liaising as necessary with the Parties to this agreement. This includes providing assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.
- Responding to data subject requests made to them in relation to the information submitted and stored in FTS, as well as requests for rectification or erasure and liaising as necessary with the Cabinet Office. This includes providing assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.
- Sharing any information in relation to which the Parties are joint controllers with any other data controllers
- Securely transferring personal data both internally and externally from the Contracting Authority.
- Review and disposal of procurement and contractual records that contain personal data as per the organisation's policies and obligations.
- Reporting any reportable data breaches within the Contracting Authority (and any connected relevant organisations to the contracting authority) in respect of personal data which is within the joint control of the Parties to their Data Protection Officer (or equivalent) and ICO within 72 hours, in consultation with the Cabinet Office.

8. **Data retention**

The Parties shall not retain or process personal data from FTS for longer than is necessary to carry out the agreed purposes 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.

9. **Agreement**

The Cabinet Office and contracting authorities signing this MoU agree that the:

- Procedures within this MoU provide an acceptable framework for the sharing of information between themselves
- The MoU is compliant with their statutory and professional responsibilities

By agreeing, the Contracting Authority undertakes responsibility for implementation of the terms of this agreement within their own organisations. Please ensure the authorised individual agreeing has taken appropriate advice from your organisation's data protection and security teams as necessary.

The agreement is to be confirmed by the authorised individual on behalf of the Contracting Authority on FTS.

This agreement has been signed by the following person from the Cabinet Office:

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

When agreement has been confirmed on CDP, the following information about the Contract Authority will be attached to this agreement:

- Name of the Contracting Authority
- Name of the person who signed
- Name of the person who provided authorisation to sign the agreement
- Job role of the person who provided authorisation to sign the agreement
- Date and time of when the agreement was agreed to on FTS.

Confirmation of this can be found within the your organisation dashboard on FTS.

The Cabinet Office will take responsibility for maintaining the list of agreeing individuals for this MoU and provide it to data subjects as requested.

Annex 1

Data Items under Joint Controllership

The personal data that Cabinet Office may collect and transfer to Contracting Authorities:

- 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 special category personal data that Cabinet Office may collect and transfer to Contracting Authorities:

- The criminal convictions data we may collect on individuals connected to the supplier relating to the 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.

CAs may also collect and transfer to CO via FTS other information under the Procurement Act 2023 and Procurement Regulations 2024.