

**Joint Schedule 11 (Processing Data)**  
Crown Copyright 2024

## **Joint Schedule 11 (Processing Data)**

### **Definitions**

1. In this Schedule, the following words shall have the following meanings and they shall supplement Joint Schedule 1 (Definitions):

**“Processor Personnel”** all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under a Contract;

### **Status of the Controller**

2. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

- (a) “Controller” in respect of the other Party who is “Processor”;
- (b) “Processor” in respect of the other Party who is “Controller”;
- (c) “Joint Controller” with the other Party;
- (d) “Independent Controller” of the Personal Data where the other Party is also “Controller”,

in respect of certain Personal Data under a Contract and shall specify in Annex 1 (*Processing Personal Data*) which scenario they think shall apply in each situation.

### **Where one Party is Controller and the other Party its Processor**

3. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller.
4. The Processor shall notify the Controller immediately if it considers that any of the Controller’s instructions infringe the Data Protection Legislation.
5. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
  - (a) a systematic description of the envisaged Processing and the purpose of the Processing;
  - (b) an assessment of the necessity and proportionality of the Processing in relation to the Deliverables;

**Joint Schedule 11 (Processing Data)**

Crown Copyright 2024

- (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
  - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
6. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:
- (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*), unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
  - (b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
    - (i) nature of the data to be protected;
    - (ii) harm that might result from a Personal Data Breach;
    - (iii) state of technological development; and
    - (iv) cost of implementing any measures;
  - (c) ensure that :
    - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
    - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
      - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
      - (B) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
      - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
      - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
  - (d) not transfer Personal Data outside of the UK or EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

**Joint Schedule 11 (Processing Data)**

Crown Copyright 2024

- (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or LED Article 37) as determined by the Controller;
    - (ii) the Data Subject has enforceable rights and effective legal remedies;
    - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
    - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
  - (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
7. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
  - (b) receives a request to rectify, block or erase any Personal Data.
  - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation.
  - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract.
  - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
  - (f) becomes aware of a Personal Data Breach.
8. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
9. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

**Joint Schedule 11 (Processing Data)**

Crown Copyright 2024

- (a) the Controller with full details and copies of the complaint, communication or request.
  - (b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation.
  - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject.
  - (d) assistance as requested by the Controller following any Personal Data Breach; and/or
  - (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
10. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
- (a) the Controller determines that the Processing is not occasional.
  - (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
  - (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
11. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
12. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
13. Before allowing any Subprocessor to Process any Personal Data related to the Contract, the Processor must:
- (a) notify the Controller in writing of the intended Subprocessor and Processing.
  - (b) obtain the written consent of the Controller.
  - (c) enter into a written agreement with the Subprocessor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Subprocessor; and
  - (d) provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.
14. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.
15. The Relevant Authority may, at any time on not less than thirty (30) Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an

**Joint Schedule 11 (Processing Data)**

Crown Copyright 2024

applicable certification scheme (which shall apply when incorporated by attachment to the Contract).

16. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than thirty (30) Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

**Where the Parties are Joint Controllers of Personal Data**

17. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11.

**Independent Controllers of Personal Data**

18. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
19. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
20. Where a Party has provided Personal Data to the other Party in accordance with paragraph 8 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
21. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
22. The Parties shall only provide Personal Data to each other:
  - (a) to the extent necessary to perform their respective obligations under the Contract;
  - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the UK GDPR); and
  - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
23. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational

**Joint Schedule 11 (Processing Data)**

Crown Copyright 2024

measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

24. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.
25. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):
  - (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
  - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
    - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
    - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
26. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
  - (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
  - (b) implement any measures necessary to restore the security of any compromised Personal Data;
  - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
  - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

**Joint Schedule 11 (Processing Data)**

Crown Copyright 2024

27. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
28. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).
29. Notwithstanding the general application of paragraphs 2 to 16 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 18 to 27 of this Joint Schedule 11.

**Joint Schedule 11 (Processing Data)**  
Crown Copyright 2024

**Annex 1 - Processing Personal Data**

This Annex shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Annex shall be with the Relevant Authority at its absolute discretion.

- 1.1 The contact details of the Relevant Authority’s Data Protection Officer are: [REDACTED], advice.dpa@hmrc.gov.uk
- 1.2 The contact details of the Supplier’s Data Protection Officer are: [REDACTED]
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p><b>The Relevant Authority is Controller and the Supplier is Processor</b></p> <p>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the Relevant Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"><li>• The data will contain the following fields (where available):<ul style="list-style-type: none"><li>○ Customer Name</li><li>○ Sector Name</li><li>○ Former directorate</li><li>○ Reporting Group Name</li><li>○ Region</li><li>○ CCM ID</li><li>○ CCM name</li><li>○ CCM email address</li><li>○ Name of customers / businesses each CCM works with</li><li>○ Tax Manager/Finance Director</li><li>○ Tax Manager/Finance Director E-Mail</li><li>○ Known Address of Business</li><li>○ Business Phone Number</li><li>○ Comments (any additional information the CCM believes the research should know before calling a business)</li><li>○ Risk status (coded so that the research contractor will not know what this variable means)</li><li>○ Alternative Business Contact Name (if known)</li></ul></li></ul>



**Joint Schedule 11 (Processing Data)**

Crown Copyright 2024

	<ul style="list-style-type: none"> <li>• The full sample will include approximately 2000 large businesses, the exact number will be confirmed nearer the time. The total numbers of participants taking part in the research is expected to be between 500 and 900 large businesses.</li> <li>• Necessary data exchange requests will be submitted to and approved by the Security and Information Business Partner (SIBP) team prior to transfer.</li> <li>• Following usual procedure, a data security plan will be completed by the research agency and approved by HMRC SIBPs.</li> <li>• Confidentiality agreements will be signed by all research agency employees on the project team and any sub-contractors who will work on the project.</li> <li>• Any sample data stored by HMRC will be stored in a secure Controlled Access Folder (CAF) accessible only by those with a business need.</li> <li>• The source of the sampled contact details is the CRMM, held by HMRC's Large Business Directorate Corporate Centre.</li> <li>• The scope of the data does not include special categories of personal data.</li> </ul>
Duration of the Processing	May 2024 to September 2027
Nature and purposes of the Processing	<p>Good customer experience is essential for healthy tax administration. HMRC needs to understand how well they are performing compared to customer expectations. This helps HMRC to tailor services and communications approaches to achieve their vision of being a trusted, modern tax and customs department. Annual customer experience and perceptions data enables HMRC to track progress against the Charter, our Customer Value Propositions, and Strategic Objectives, including attitudes to compliance.</p>

**Joint Schedule 11 (Processing Data)**  
Crown Copyright 2024

	<p>The large business survey was established in 2015 and has provided robust measures of customer experience and perceptions of HMRC for this key customer group. Thematic coverage gives ExCom, internal and external stakeholders high-level credible evidence. This can be used to help HMRC identify positive experiences and areas where improvements are required. We are seeking to continue the Large Business survey for 3 more years.</p> <p>This will require contracting an external research agency to conduct the research. Capturing large businesses’ perceptions of HMRC’s reputation, informs tailored communication approaches that support HMRC’s vision to be a trusted, modern tax and customs department. These ongoing needs can only be met via a large-scale survey.</p> <p>The Large Business survey offers unique insight into how HMRC is viewed as an organisation, by providing a customer experience perspective and tracking reputational factors over the previous 12-months. Including qualitative research allows us to develop our understanding of what lies behind customers’ ratings to provide more specific evidence on where we should focus efforts to improve performance. The survey results are reviewed at high-level internal forums, such as ExCom and the Customer Experience Committee to provide assurance on the impact of departmental decisions on customer experience and direction of travel. They also inform HMRC’s communications strategy which supports HMRC’s operational focus and service transformation. Other means would not be viable to achieve this function.</p> <p>The Large Business survey provides a robust source of customer experience and perception data for this customer group which is not available through HMRC customer data, other research projects or from transactional exit surveys. The robust methodological approach is essential to enable annual external reporting of trends.</p> <p>HMRC have commissioned IFF Ltd ( a research contractor) to undertake the survey.</p> <div></div> <div></div>
--	--

**Joint Schedule 11 (Processing Data)**

Crown Copyright 2024

Type of Personal Data	<p>The data will be largely corporate but will contain the following types of personal data,</p> <ul style="list-style-type: none"> <li>• Customer Name</li> <li>• CCM ID</li> <li>• CCM name</li> <li>• CCM email address</li> <li>• Tax Manager/Finance Director</li> <li>• Tax Manager/Finance Director E-Mail</li> <li>• Alternative Business Contact Name (if known)</li> </ul>
Categories of Data Subject	The full population of large businesses managed by HMRC's Large Business Directorate (LBD).
<p>Plan for return and destruction of the data once the Processing is complete</p> <p>UNLESS requirement under Union or Member State law to preserve that type of data</p>	<p>We will determine IFF LTd's (the research contractor) retention policy to ensure it does not exceed twelve months. Files that have not been opened for longer than twelve months should be automatically deleted to ensure data is not kept longer than required. We will request that the research contractor will provide written confirmation to HMRC of deletion of the sample files. Data collected during the fieldwork will be retained until reporting is concluded in the final year of the project, but final milestone payments will only be approved when this data is deleted.</p>

**Joint Schedule 11 (Processing Data)**  
Crown Copyright 2024