***Template Controller-Processor Clause***

**IMPORTANT NOTICE: This document is issued in association with the ICAS Guide – 'Preparing for GDPR' - and is issued subject to the terms of the disclaimer contained within that Guide.**

**This is an example of a clause and accompanying Schedule which could be inserted into a contract where a party (the processor) is processing data on behalf of another party (the controller).**

|  |
| --- |
| **General Notes to users:**   1. **This is a short form clause which can be incorporated into a general commercial agreement.** 2. **The clause is intended to be broadly balanced in terms of the respective rights and obligations of the parties. In some places, pro-controller and pro-processor options are included.** 3. **This drafting uses the term [Party 1] to refer to the customer or purchaser under the wider contractual arrangement of which the Clause and Schedule forms part. The term is just a placeholder – the term should be substituted in favour of the defined term used in the rest of the agreement to describe the customer/purchaser.** 4. The drafting assumes that [Party 1] is a controller and [Party 2] is merely a processor of the Disclosed Data. 5. Delete the drafting notes from the drafting when it is inserted into an agreement. |

Definitions and Interpretation [Note: Include these definitions within the clause in the wider agreement which contains the agreement definitions.]

**"Controller"** has the meaning given to that term in Data Protection Law;

**"Data Subject"** means an individual who is the subject of any of the Disclosed Data.

**"Data Subject Request"** means a written request of [Party 1] by or on behalf of a Data Subject to exercise any rights conferred by Data Protection Law;

**"Disclosed Data"** means the Personal Data disclosed to [Party 2] by or on behalf of [Party 1] in connection with the Purpose, comprising [*insert high level* *description of the types of Personal Data and categories of Data Subject – eg customers, employees*];

**"Data Protection Law"** means any laws or regulations that apply from time to time to the Processing of Personal Data by either Party under this Agreement and to include the EU Data Protection Directive 95/46/EC, the EU Privacy & Electronic Communications Directive 2002/58/EC, Regulation (EU) 2016/679 (if and from the date that it enters into force in the United Kingdom), all national implementing legislation (including, without limitation, the Data Protection Act 1998) and subordinate legislation in the United Kingdom and any applicable decisions and guidance made under them; **[*Note: this clause should be updated once GDPR is in force and the Data Protection Act 1998 is repealed. Once the current Data Protection Bill becomes an Act of Parliament[[1]](#footnote-1), the reference to the 'Data Protection Act 1998' can be changed to the 'Data Protection Act 2018'.*]**

**"European Economic Area"** means the member states of the European Economic Area, from time to time, and for the purposes of this Agreement will include the United Kingdom notwithstanding any departure of the United Kingdom from the European Economic Area;

**"Personal Data"** and **"Processing"** each have the meanings given to them in Data Protection Law and **"Process"** and any other tense or part of that verb will be interpreted accordingly;

**"Processor"** has the meaning given to that term in Data Protection Law; and

**"Purpose"** means [*describe the purpose of the processing*]*.*

1. Data Protection
   1. [Party 1] and [Party 2] acknowledge that, for the purposes of Data Protection Law, [Party 1] is the Controller and [Party 2] is the Processor of any Disclosed Data. Each party will comply with its obligations under Data Protection Law.
   2. [Party 1] warrants and represents that the Processing of the Disclosed Data instructed by [Party 1] under this Agreement is lawful. **[*Note: a processor may seek an indemnity for non-compliance by the controller. However, doing that then makes it difficult to resist a reciprocal indemnity for a processor breach. Consider on a case by case basis.*]**
   3. [Party 2] will Process the Disclosed Data only to the extent, and in such a manner, as is necessary for the Purpose, subject to and in accordance with [Party 1]’s express written instructions from time to time. If [Party 2] considers that any instruction from [Party 1] contravenes Data Protection Law, it shall notify [Party 1], giving reasonable details.
   4. In accordance with its obligations under Data Protection Law, [Party 2] will implement appropriate technical and organisational measures so as to ensure an appropriate level of security is adopted to mitigate the risks associated with the Processing of such Disclosed Data. Those measures may include, where appropriate, pseudonymising and encrypting Disclosed Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Disclosed Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it. [Upon the request, [[Party 2] shall provide [Party 1] with a description of such measures.] **[*Note: this clause takes a short form approach to the security obligations required by GDPR. The obligation to provide information on the measures is optional drafting. Controllers should, however, be reviewing those measures as part of their supplier diligence and may also require specific details to be included or expressly referenced in the Agreement.*]**
   5. [Party 2] will:
      1. at [Party 1][*or*] [Party 2]’s cost and expense:
         1. promptly comply with any request from [Party 1] requiring [Party 2] to update or otherwise amend, transfer, delete or destroy the Disclosed Data, provided that [Party 2] will not be in breach of any other obligation under this Agreement to the extent that [Party 2] cannot perform that obligation as a result of its compliance with this Clause 1.5.1.1;
         2. assist [Party 1] to the extent reasonably required in responding to any relevant Data Subject Request; and
         3. without prejudice to Clauses 1.5.1.1 and 1.5.1.2, assist [Party 1] to the extent that such assistance is necessary to enable [Party 1]’s compliance with its obligations under Data Protection Law in relation to the Processing of the Disclosed Data by [Party 2] under this Agreement, such assistance having regard to the nature of the Processing and the information available to [Party 2];
      2. ensure that the Disclosed Data is Processed only by employees, contractors or other personnel that are subject to an appropriate duty of confidentiality:
      3. not transfer any of the Disclosed Data outside the European Economic Area, except upon and in accordance with the express written instructions or agreement in writing of the [Party 1] **[*Note: this is short form wording, but if the processor envisages at the outset that there will be transfers of Personal Data outside the EEA then the clause should provide for that (using a similar model to the sub-processor wording below).*]**
   6. **[OPTION 1 – PRO-CONTROLLER]** Notwithstanding any other provision of the Agreement, [Party 2] shall not without [Party 1]’s prior written consent, which consent [Party 1] may give or withhold in its entire discretion and, where given, be made subject to conditions sub-contract any of its obligations in relation to the Processing of the Disclosed Data or otherwise authorise any third party to Process Disclosed Data on its behalf (except to the extent a specific third party has been approved for this purpose in writing by [Party 1]).

[OR]

**[OPTION 2 – PRO-PROCESSOR]** [Party 1] acknowledges that [Party 2] may utilise sub-processors in connection with the Processing of the Disclosed Data (each a **“Sub-Processor”**). [Party 2] shall maintain a record of any Sub-Processors that are utilised or otherwise contemplated by [Party 2] from time to time and shall impose obligations on that Sub-Processor substantially equivalent to those applying to [Party 2] under this Clause 1. [Party 1] authorises the use of the following as a Sub-Processor:

* + 1. [●]

provided that where there is an addition or replacement of any Sub-Processor referred to in Clause [1.6.1], [Party 2] shall inform [Party 1] in advance of any such intended changes. If [Party 1], acting reasonably, objects in writing to such addition or replacement, the parties shall discuss in good faith [Party 1]’s concerns and [Party 2] shall use reasonable efforts to make a change to the affected Services or to propose a commercially reasonable change that avoids the need to utilise that Sub-Processor. If [Party 2] is unable to implement such a change within [●] days of receipt of [Party 1]’s objection, then [Party 1] acknowledges that its sole remedy is to terminate this Agreement (in respect of those affected [Services] only) on not less than [●] days’ notice in writing. **[*Note: GDPR requires that a controller has a right to object to new/replacement sub-processors. This clause sets out one way to deal with that right, without giving a right of veto over the processor’s business model. If the controller does not agree with the sub-processing then its remedy is a right of termination. This needs to align with the processor’s standard position on sub-contracting generally.*]**

* 1. Except to the extent that [Party 2] is required by law to retain any copies of any Disclosed Data, upon the expiry or termination of this Agreement [Party 2] will deliver to [Party 1] or destroy and/or permanently delete from its information technology systems all copies of any Disclosed Data in its possession.
  2. **[OPTION 1 – PRO-CONTROLLER]** [Party 2] shall (at its own cost and expense) provide [Party 1] with such information in [Party 2]’s possession and permit [Party 1] (or any auditor appointed by [Party 1]) to have access to [Party 2's] premises, personnel and records, on reasonable notice, to the extent reasonably required for verifying compliance with Data Protection Law and the requirements of this Agreement.

**[OPTION 2 – PRO-PROCESSOR]** At [Party 1]’s cost and expense, [Party 2] will:

* + 1. provide [Party 1] with such information in [Party 2]’s possession; and
    2. permit [Party 1] a reasonable right of audit in relation to [Party 2]’s policies and procedures relating to the Processing of Disclosed Data under this Agreement.**[*N*ote*: GDPR requires that Controllers have a right of audit. This should be aligned with any controls in the general audit provisions (if any) in the contract (option 1). If there is no general audit clause then use option 2. The extent of the audit right will depend on the nature of the contract. The wording here is short form. Some clients may expect more detailed rights.*]**

in each case as is reasonably necessary to enable [Party 1] to demonstrate its compliance with Data Protection Law in connection with this Agreement.

* 1. Nothing in this Agreement relieves either party of its own direct responsibilities and liabilities under Data Protection Law.

1. For up to date information on the progress of the Bill please visit the UK Parliament website page [here](https://services.parliament.uk/bills/2017-19/dataprotection.html). [↑](#footnote-ref-1)