Joint Controller Agreement
Data Processing Agreement
(Standard)

Background

A. New data protection legislation came into force during 2018, which aims to protect the privacy of all EU citizens and prevent data breaches. It will apply to any public or private organisation processing personal data. Established key principles of data privacy remain relevant in the new Data Protection Legislation but there are also a number of changes that will affect commercial arrangements, both new and existing, with suppliers.

B. The Data Protection Legislation comprises: i) the General Data Protection Regulation (GDPR) 25 May 2018; and ii) the Data Protection Act (DPA) 2018.

C. The GDPR applies to 'Controllers' and 'Processors'. These definitions are broadly the same as under the Data Protection Act 2018 i.e. the Controller says how and why personal data is processed and the Processor acts on the Controller's behalf. Contracts currently subject to the DPA 1998 will also to be subject to the GDPR.

a) ***Personal Data*** means any information that relates to an identified or identifiable living subject i.e. staff member, member of the public, customer, etc. It will generally include an individual's name, address, phone number, date of birth, place of work, dietary preferences, opinions, opinions about them, whether they are members of a trade union, their political beliefs, ethnicity, religion, or sexuality. It can also include an individual's email address or job title if that sufficiently picks them out so that they can be identified (in isolation or with other information that may be held). The above is not exhaustive and any information that relates to an individual can be personal data.

b) a ***Controller*** is a natural or legal person or organisation which determines the purposes and means of processing personal data. In this agreement the Controller is the client

c) a ***Processor*** is a natural or legal person or organisation which processes personal data on behalf of a Controller.

d) **Joint Controller** a situation when in our capacity as Chartered Accountants Beckingtons act together with the Controller [Client], to decide the purposes and manner of data processing such as collecting and sharing data with third parties for your Legitimate Interests of for Legal purposes

D. In the Agreement, Beckingtons is a supplier of services to [Client] that involves the processing of Personal Data on behalf of [Client], for the purposes of processing Personal Data, [Client] is the Controller and Beckingtons is the **Joint Controller** when processing personal data.

E. [Client] and Beckingtons now agree that from the 25th May 2018 this Addendum shall come into effect and shall replace all clauses in the Agreement relating to Data processing:

DEFINITIONS

Affiliate means any entity that directly or indirectly controls, is controlled by, or is under common control with another entity;

Controller Personal Data means all Personal Data which is owned, controlled or processed by Controller and which is provided by or on behalf of Controller to the Processor or which comes into the possession of the Processor as a result of or in connection with the supply of the Services;

Data Controller, Data Processor, Data Subject, Personal Data and **Processing** shall bear the respective meanings given to them in the Data Protection Act 1998 or General Data Protection Regulation 2016 (as applicable) (in each case as may be amended, updated, replaced or superseded from time to time) (and **Process** and **Processes** shall be construed accordingly);

Data Protection Law means the EU Data Protection Directive 95/46/EC, the Data Protection Act 2018 and any other legislation in force from time to time which implements that Directive, the Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699), the Electronic Communications Data Protection Directive (2002/58/EC), the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003) and any laws that replace or amend any of these (including without limitation the General Data Protection Regulation 2016 (Regulation (EU) 2016/679) (**GDPR**)), together with the equivalent legislation of any other applicable jurisdiction and all other applicable law, regulations, guidance and codes of conduct in any relevant jurisdiction relating to the processing of personal data and privacy including the guidance and codes of practice issued by the Information Commissioner's Office (**ICO**), the Article 29 Working Party, the European Data Protection Board or any other relevant supervisory authority from time to time;

Description of Processing means the description of Processing as set out in the Agreement;

Good Industry Practice means the exercise of that degree of skill, diligence, prudence, foresight and operating practice which, at the relevant time, would reasonably and ordinarily be expected from a skilled and experienced person engaged in the same or a similar business;

Group means in relation to a company, that company, any subsidiary or holding company from time to time of that company, and any subsidiary from time to time of a holding company of that company;

Group Company means in relation to a company, any member of its Group;

1. Law and Security

1.1. The parties agree that [Client] is a Controller and instructs Beckingtons regarding the purposes and means of processing personal data pursuant to this Agreement. However, in their capacity as Accountants there may be legitimate reasons when Beckingtons will process personal data without instruction from [Client] and act as Joint Controller. Beckingtons are therefore defined as a Joint Controller for the purposes of this agreement

1.2. The Joint Controller shall:

(a) implement appropriate technical and organisational measures to protect Controller Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data Processed by it.

(b) preserve so far as possible the security of Controller Personal Data and prevent any loss, disclosure, theft, manipulation or interception of Controller Personal Data; and

(c) ensure that its anti-malware controls are deployed and maintained in accordance with Good Industry Practice and any of the Joint Controller's IT policies, check for and delete any malicious materials from its systems and not intentionally or negligently transfer any malicious materials onto any of the Controller's IT systems or onto any media containing Controller Personal Data.

(d) The Joint Controller shall provide to the Controller at any time on request a detailed written description of such technical and organisational measures in place.

2. Sub-processing and transfer

2.1. The Joint Controller shall not permit any Processing of Controller Personal Data by any agent or subcontractor or other third party ("Sub-Processor") without providing the Controller with such information as the Controller may require in this respect and receiving the prior written authorisation of the Controller and only then subject to such conditions as the Controller may require and provided that the Joint Controller remains fully liable for all the actions and omissions of the Sub-Processor and that any Sub-Processor agrees in writing to comply with obligations the same as those imposed on the Joint Controller in this Schedule 4.

3. Instructions and Transfer

3.1. The Joint Controller or any of its employees, staff, workers, agents or consultants ("Processor Personnel") shall:

(a) only Process the Controller Personal Data for the purposes of supplying the Services (and for no other purpose whatsoever), and at all times in accordance with Good Industry Practice, the Controller's documented instructions from time to time, the Controller's Data Protection Policies, the Description of Processing and all applicable Data Protection Laws; and

(b) not transfer, or otherwise directly or indirectly disclose, any Controller Personal Data to countries outside the European Economic Area (EEA) without the prior written consent of the Controller (which may be refused or granted subject to such conditions as the Controller deems necessary) except where the Joint Controller is required to transfer the Controller Personal Data by the laws of the member states of the EU or EU law (and shall inform the Controller of that legal requirement before the transfer, unless those laws prevent it doing so). If, at any time, the United Kingdom is not in the EEA, the Joint Controller may transfer any Controller Personal Data to the United Kingdom provided that the United Kingdom has been deemed an adequately protective jurisdiction for the purposes of the applicable Data Protection Law and until and unless the United Kingdom has been deemed adequately protective, the Joint Controller shall only transfer Controller Personal Data to or Process such data in the United Kingdom provided it enters into all further terms (whether with the Controller or any other party) and completes, maintains and implements (as applicable) all other actions, measures and safeguards as required to ensure that such transfers and Processing do not breach the obligations of the Joint Controller or the Controller [or the Controller's Affiliates] under Data Protection Law, including, if applicable, the valid execution of the EU model contractual clauses as set out in Decision 2010/87/EU (or, at the

Controller's option, any alternative version of those clauses issued by the European Commission or a supervisory authority from time to time).

4. Personnel

THE JOINT CONTROLLER SHALL:

(a) ensure that access to Controller Personal Data is limited to the Joint Controller Personnel and authorised Sub-Processors who need access to it to supply the Services, and that all Joint Controller Personnel and authorised Sub-Processors are: informed of the confidential nature of Controller Personal Data, and that they must not disclose the Controller Personal Data;

(b) are subject to an enforceable obligation of confidence with regards to the Controller Personal Data; and

(c) are assessed by the Joint Controller or authorised Sub-Processor prior to any Processing of Controller Personal Data to ensure their reliability, and that they receive training on data protection matters.

5. Security – Technical and Organisational Measures

5.1. The Joint Controller shall implement appropriate technical and organisational measures to protect Controller Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data Processed by it, including (inter alia) where appropriate
:

(a) encryption of the Controller Personal Data;

(b) guaranteeing the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) restoring the availability and access to the Controller Personal Data in a timely manner in the event of a physical or technical incident; and

(d) regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing.

(e) The Joint Controller shall provide to the Controller at any time on request a detailed written description of such technical and organisational measures in place.

6. Data Subject Rights

6.1. The Joint Controller or any of its Joint Controller Personnel shall promptly provide such information and assistance (at no cost to the Controller) as the Controller may require in relation to any request from or on behalf of any Data Subject for access, rectification or erasure of Controller Personal Data, or any complaint, objection to Processing, or other correspondence. In no event shall the Joint Controller or any of the Joint Controller Personnel respond directly to any such request, complaint or correspondence without the Controller's prior written consent unless and to the extent required by law;

7. Data Security, Breach Reporting and DPIAs

7.1. The Joint Controller or any of its Personnel shall:

(a) immediately (and in any event within 2 calendar days) and fully notify the Controller in writing if any Controller Personal Data has been disclosed in breach of this clause or if it is lost, becomes corrupted, is damaged or is deleted in error.

7.2. The Joint Controller shall notify the Controller immediately if it suspects or becomes aware of any actual, threatened or potential breach of security of Controller Personal Data and any personal data breach (as defined in the GDPR) and shall ensure all such notices include full and complete details relating to such breach, in particular:

(a) the nature and facts of such breach including the categories and number of Controller Personal Data records and, if applicable, Data Subjects concerned;

(b) the contact details of the data protection officer or other representative duly appointed by the Joint Controller from whom the Controller can obtain further information relating to such breach;

(c) the likely consequences or potential consequences of such breach; and

(d) the measures taken or proposed to be taken by the Joint Controller and/or any Joint Controller Personnel to address such breach and to mitigate any possible adverse effects and the implementation dates for such measures.

7.3. The Joint Controller or any of its Personnel shall:

(a) promptly provide such information and assistance (at no cost to Controller) as the Controller may require in relation to:

(b) the Controller's decision to undertake a data protection impact assessment where the Controller considers (in its sole discretion) that the type of Processing may result in a high risk to the rights and freedoms of Data Subjects.

7.4. The Joint Controller or any of its Personnel shall:

(a) promptly provide such information and assistance (at no cost to Controller) as the Controller may require in relation to:

(b) any approval of the Information Commissioner or other data protection supervisory authority to any Processing of Controller Personal Data, or any request, notice or investigation by such supervisory authority.

8. Personal data – return or destruction

8.1. The Joint Controller or any of its employees, staff, workers, agents or consultants ("Processor Personnel") shall:

(a) on request at any time and on the expiry or termination of this Agreement (and/or specific services within it), (at no cost to the Controller) at the Controller's option either return all of the Controller Personal Data, and/or Confidential Information, and copies of it in such format as the Controller may require or securely dispose of the Controller Personal Data and/or Confidential Information except to the extent that any applicable law requires the Joint Controller to store such Controller Personal Data and the Joint Controller has promptly demonstrated their legal requirements to the reasonable satisfaction of the Controller

(b) the Joint Controller shall ensure at all times that Controller personal data is maintained in accordance with any specified data retention requirements.

9. Audit

9.1. The Joint Controller shall permit the Controller (and any of its authorised representatives) and the Information Commissioner (or its authorised representatives), at the Joint Controller 's cost, access to any of the Joint Controller 's premises, personnel, IT systems and relevant records as may be reasonably required by the Controller upon reasonable notice at any time for the purposes of conducting an audit in order to verify the Joint Controller's compliance with this clause [insert reference to entire data protection clause] and Data Protection Laws.

9.2. The Joint Controller shall, on demand, provide the Controller and the Information Commissioner (and/or their authorised representatives) with all reasonable co-operation, access and assistance in relation to each audit.

9.3. The Joint Controller shall permit and contribute to all audits or inspections conducted by the Controller and/or the Information Commissioner (or their authorised representatives) for the purpose of confirming the Joint Controller 's compliance with this clause and the Data Protection Laws.

9.4. In the Joint Controller 's reasonable opinion, to the extent that it believes that any instruction received by it is likely to infringe the Data Protection Law or any other applicable law, the Joint Controller shall promptly inform the Controller.

10. Provision of Controller Personal Data by Joint Controller to Controller

10.1. To the extent that the Joint Controller collects and passes Personal Data to the Controller pursuant to this Agreement, it represents, warrants and undertakes that:

(a) it has obtained appropriate authority from all Data Subjects to whom it relates, or has provided them with the requisite information required under the Data Protection Law, to pass their Personal Data to the Controller for the purposes for which the Controller intends to use it and/or as specified by the Controller in writing; and

(b) it is accurate and up to date.

11. Readiness of equipment and systems to meet rapid timescales

11.1. The Joint Controller shall ensure that any equipment or systems used to store Controller Personal Data is capable of providing such data:

(a) to the Controller or any of its Affiliates;

(b) directly to a Data Subject; or

(c) to any data controller specified by a Data Subject,

in each case, in a structured, commonly used and machine-readable format within 2 Business Days of the Controller's written request and, in respect of (b) and (c), only in accordance with the Controller's written instructions.

12. Remedying a breach

12.1. If the Joint Controller breaches or potentially breaches its obligations set out in this clause or there occurs any threat to the security of the Controller Personal Data, the Joint Controller shall:

(a) take immediate steps to remedy the breach or prevent the potential breach or remove the threat;

(b) promptly take measures to ensure there is no repetition of the incident in the future;

(c) promptly provide the Controller with full details in writing of the steps and measures taken; and

(d) comply (at no cost to the Controller) with all requests made by the Controller in respect of the breach or threat.

13. Data restoration/ recreation

13.1. The Joint Controller shall (at no cost to the Controller) restore or recreate (in a timely manner and in accordance with Good Industry Practice) all Controller Personal Data which is lost, deleted or corrupted by the Joint Controller or any of the Joint Controller Personnel in breach of this clause.

14. Record keeping

14.1. The Joint Controller shall keep detailed, accurate and up-to-date records relating to its Processing of Controller Personal Data, and shall make available to the Controller on request (at no cost to the Controller) all information necessary to demonstrate compliance with the obligations laid down in this clause.

15. Compliance with data protection law

15.1. The Joint Controller shall supply the Services in such a way as to ensure compliance with all Data Protection Law and this clause and shall not place the Controller in breach of Data Protection Law. The Joint Controller shall demonstrate to the Controller no later than [date] that it is ready to comply with GDPR from 25 May 2018.

16. Security and back-up systems

16.1. The Joint Controller shall at all times comply with ISO/IEC27001 or otherwise comply with Good Industry Practice relating to data protection, and implementation and maintenance of back-up systems and the Business Continuity Plan.

17. Security and penetration testing

17.1. The Joint Controller shall at all times ensure that its IT systems are fit for the purpose of securing Controller Personal Data in accordance with Good Industry Practice and this Agreement and are regularly maintained and, if necessary, upgraded to ensure this.

17.2. Where the Joint Controller, as part of the Services, provides the Controller with access to any IT system or stores any Controller Personal Data on its own systems or any systems of any Affiliate, Sub-Processor or contractor, the Joint Controller shall, at its own cost, undertake annual application and/or infrastructure level penetration testing using a United Kingdom based independent CREST certified contractor and provide the Controller with details of the results of such tests. Remedial actions identified by such penetration testing shall be undertaken by the Joint Controller at the Joint Controller's cost.

18. Disposal of personal data

18.1. The Joint Controller shall ensure that if any Controller Personal Data is disposed of, such disposal takes places in a secure manner such that the Controller Personal Data is not recoverable.

19. Personnel

19.1. The Joint Controller or any of its employees, staff, workers, agents or consultants ("Joint Controller Personnel") shall comply fully with the Data Protection Laws and not, by any act or omission, cause the Controller to breach any Data Protection Law.

20. Indemnity

20.1. Any person who has suffered material or non-material damage as a result of an infringement of their personal data has the right to receive compensation for the damage suffered.

20.2. As a Joint Controller Beckingtons shall only be liable for the damage caused by processing only where it has not complied with obligations of the GDPR Regulation or where it has acted outside or contrary to lawful instructions of the controller [Client]

Change History

Signed

Date: 2/4/2019

Change History

Issue Number	Issue Date	Comments
1.1	23/10/18	Cyber Essentials Certification
1.2	2/4/19	GDPR Fundamentals Project