

S

A

(1) <er>>

(2) <or>>

M

DATA MENT

P

L

E

THIS AGREEMENT is made the
BETWEEN:

- (1) <<Name of Data Controller>> incorporated in <<Country of Registration>> under number <<Company Number>> whose registered office is at] **OR**
[of] <<insert Address>> (“Data Controller”)
- (2) <<Name of Data Processor>> incorporated in <<Country of Registration>> under number <<Company Number>> whose registered office is at] **OR**
[of] <<insert Address>> (“Data Processor”)

WHEREAS:

- (1) [Under a written agreement dated <<insert date>> (“the Agreement”) the Data Processor provides to the Data Controller] **OR** [The Data Processor to provide to the Data Controller the services described in Schedule 1.
- (2) The provision of the Services by the Data Processor involves it in processing the Personal Data described in Schedule 1 on behalf of the Data Controller.
- (3) Article 28(3) of the retained EU law (the “GDPR”) ((EU) 2016/679) (the “UK GDPR”) requires the Data Controller and any organisation acting on its behalf to enter into a written agreement in writing between the Data Controller and any organisation acting on its behalf, which sets out the measures to be taken by the Data Processor to ensure compliance with the provisions of the UK GDPR governing the processing of Personal Data on its behalf,
- (4) The Parties have agreed to enter into this Agreement to ensure compliance with the provisions of the UK GDPR governing the processing of the Personal Data by the Data Processor for the purposes of the Services.
- (5) The terms of this Agreement shall apply to all processing of Personal Data carried out for the Data Controller and to all Personal Data held by the Data Processor in relation to the Services.

IT IS AGREED as follows:

1. Definitions and Interpretation

- 1.1 In this Agreement, unless otherwise requires, the following expressions have the meanings set out below:

“Data Controller”

the person or entity given to the term “controller” in the GDPR; or the Data Protection Act 2018;

“Data Processor”

the person or entity given to the term “processor” in the GDPR; or the Data Protection Act 2018;

- a) "any" includes a reference to any reference made by electronic or facsimile transmission or otherwise;
- b) "reference to a statute" is a reference to that statute or to that statute as amended or re-enacted at the relevant time;
- c) "reference to this Agreement" is a reference to this Agreement and each of the Schedules or supplemented at the relevant time;
- d) "reference to a Clause" is a reference to a Clause of this Agreement (including the Schedules) or a paragraph of the relevant Schedule;
- f) "Parties" refer to the parties to this Agreement.
- 1.3 The Schedules to this Agreement are for convenience only and shall have no effect if they conflict with the provisions of this Agreement.
- 1.4 Words in the singular shall include the plural and vice versa.
- 1.5 References to gender shall include any other gender.
- 1.6 References to "person" shall include corporations.
- 2. Scope and Application of this Agreement**
- 2.1 The provisions of this Agreement shall apply to the processing of the Personal Data of the Data Subject, carried out for the Data Controller by the Data Processor in relation to all such Personal Data held by the Data Processor in relation to the Data Subject at the date of this Agreement.
- 2.2 [The provisions of this Agreement shall be deemed to be incorporated into the Service Agreement expressly set out in it. Subject to sub-Clause 2.3, the provisions of this Agreement shall apply to the Service Agreement.]
- 2.3 In the event of any ambiguity between any of the provisions of this Agreement and any other agreement between the Parties, the provisions of this Agreement shall prevail.
- 2.4 In the event of any ambiguity between any of the provisions of this Agreement and the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses will prevail.
- 3. Processing of Personal Data**
- 3.1 The Data Processor shall process the Personal Data of the Data Subject in accordance with the purpose(s) of Personal Data, the category or categories of Personal Data, the processing to be carried out, the purpose(s) of the processing.
- 3.2 Subject to the provisions of this Agreement, the Data Processor is only to carry out the processing of the Personal Data received from the Data Controller for the purposes of the Services and not for any other purpose;
- a) The Data Processor shall process the Personal Data in a manner as is necessary for those purposes;

S

c) shall comply with the express written authorisation and instructions of the Data Controller (which may be specific instructions of a general nature or as otherwise notified by the Data Processor).

3.3 The Data Processor shall maintain control of the Personal Data at all times and ensure its compliance with the relevant Data Protection Legislation. The Data Processor shall be limited to, its collection, holding, and processing of the Personal Data in place all necessary and appropriate consents and shall not transfer the Personal Data to the Data Processor or to any other third party without the written instructions given to the Data Controller.

4. The Data Processor

4.1 As set out in clause 3, the Data Processor shall only process the Personal Data and in such a manner as is necessary for the purposes specified in the instructions given by the Data Controller and not for any other purpose. All instructions given to the Data Processor shall be made in writing and shall comply with the Data Protection Legislation. The Data Processor shall follow such written instructions from the Data Controller unless prohibited from doing so by law (as per Article 6(1)(c) of the Data Protection Act 2018 (in which case, the Data Processor shall inform the Data Controller of the legal requirement in question before processing the Personal Data unless prohibited from doing so by law).

4.2 The Data Processor shall not process the Personal Data in any manner which contravenes the provisions of this Agreement or with the Data Protection Legislation. The Data Processor must inform the Data Controller immediately if, in its opinion, any instructions given by the Data Controller conflict with the Data Protection Legislation.

4.3 The Data Processor shall promptly comply with any written request from the Data Controller to amend, transfer, delete (or otherwise process) the Personal Data.

4.4 The Data Processor shall promptly comply with any written request from the Data Controller to stop, mitigate, or remedy any breach involving the Personal Data.

4.5 The Data Processor shall provide all reasonable assistance [(at its own cost)] to the Data Controller in complying with its obligations under the Data Protection Legislation including, but not limited to, the Data Controller's obligations to protect subjects' rights, the security of processing, the prevention of data breaches, the conduct of data protection impact assessments with the Information Commissioner (including, but not limited to, consultations with the Information Commissioner where a data protection impact assessment indicates that there is a high risk which requires consultation with the Information Commissioner).

4.6 For the purposes of clause 4.5, "all reasonable assistance" shall take into account the nature of the processing carried out by the Data Processor and the instructions given to the Data Processor.

4.7 In the event that the Data Processor becomes aware of any changes to the Personal Data that may, in its reasonable interpretation, affect the performance of the Services and the processing of the Personal Data, the Data Processor shall inform the Data Controller [under this Agreement,

A

M

P

L

E

the Data Processor shall inform the Data Controller promptly.

5. **Confidentiality**

5.1 The Data Processor shall maintain the Personal Data in confidence, and in particular shall not disclose the Personal Data to any third party unless the Data Controller has given written consent for the Data Processor to do so. The Data Processor shall not process or make any use of any Personal Data for any purpose other than that specified by the Data Controller otherwise than as necessary for the provision of the Services to the Data Controller.

5.2 Nothing in this clause shall prevent the Data Processor from complying with a legal obligation to disclose or process Personal Data where such disclosure or processing is required by domestic law, court, or regulator (including the Information Commissioner). In such cases, the Data Processor shall notify the Data Controller of the disclosure or processing prior to disclosure or processing (unless such notification is required by domestic law) in order that the Data Controller may wish to do so.

5.3 The Data Processor shall ensure that all employees who are to access and/or process Personal Data are informed of its confidential nature and shall keep the Personal Data confidential.

6. **Employees and Data Protection Officer[s]**

6.1 [The Data Controller has appointed a data protection officer in accordance with Article 37(2) of the GDPR, whose details are as follows: <<insert name and contact details>>.]

6.2 [The Data Controller has appointed a data protection officer in accordance with Article 37(2) of the GDPR, whose details are as follows: <<insert name and contact details>>.]

OR

6.2 [The Data Controller shall appoint a data protection officer in accordance with Article 37(2) of the GDPR and shall supply the details of the data protection officer to the Data Controller prior to the commencement of the processing of Personal Data.]

6.3 The Data Processor shall ensure that all employees who are to access and/or process Personal Data are given suitable training on the Data Processor's obligations under it, their application to their work, with particular regard to the processing of Personal Data under this Agreement.

7. **Security of Processing**

7.1 The Data Processor shall implement appropriate technical and organisational measures (such as encryption, pseudonymisation, anonymisation, access controls, etc.) approved by the Data Controller and] **OR** [,] as may be required by law to take all steps necessary to protect the Personal Data against loss, destruction, unlawful processing or accidental or unlawful loss, destruction, or disclosure. The Data Processor shall inform the Data Controller of any changes to such measures.

- 7.2 The measures adopted by the Data Processor shall be appropriate to the nature of the Personal Data, to the harm that may result from such processing or accidental or unlawful loss, destruction or damage, in particular to the rights and freedoms of Data Subjects and in regard for the state of technological development and time.
- 7.3 The measures adopted by the Data Processor may include, as appropriate, the pseudonymisation and encryption of the Personal Data; the ability to ensure the confidentiality, integrity, availability, and resilience of processing operations; the ability to restore the availability of and access to the Personal Data in a timely manner in the event of a physical or technical failure; the process for regularly testing, assessing, and evaluating the effectiveness of the technical and organisational measures.
- 7.4 The Data Processor shall also requested by the Data Controller (and within the time frame requested by the Data Controller) supply further details of the technical and organisational measures in place to safeguard the security of the Personal Data and to prevent unauthorised access.
- 7.5 [The Data Processor shall document all technical and organisational measures and shall review them on a <<insert frequency>> basis to ensure they remain appropriate and up to date.]
8. **Data Subject Rights**
- 8.1 The Data Processor shall take appropriate technical and organisational measures to ensure that it is able to provide reasonable assistance [(at its own cost)] **OR** [(at the request of the Data Controller in complying with its obligations under the applicable legislation with particular regard to the following:
- a) to enable Data Subjects under the Data Protection Legislation to exercise, in particular, the right of access (data subject access request), the right to rectification, the right to erasure, portability rights, the right to object to processing, rights relating to automated decision making and to restrict processing; and
 - b) to ensure that the Data Controller by the Data Processor pursuant to the Data Protection Legislation.
- 8.2 In the event that the Data Processor receives any notice, complaint, or other communication from a Data Subject relating to the Personal Data processing or to either Party's obligations under the Data Protection Legislation, it shall notify the Data Controller of such communication.
- 8.3 In the event that the Data Processor receives any request from a Data Subject relating to the Personal Data processing or to either Party's obligations under the Data Protection Legislation including, but not limited to, a data subject access request, it shall notify the Data Controller of such request without undue delay].
- 8.4 The Data Processor shall cooperate fully [(at its own cost)] **OR** [(at the request of the Data Controller and provide all reasonable assistance in relation to any complaint, notice, other communication, or request received by:
- a) the Data Controller with full details of the complaint or request;
 - b) the Data Controller with any information and assistance in order to comply with the request;

- c) [redacted] controller with any Personal Data it holds in relation [redacted] (within the timescales required by the Data [redacted])
- d) [redacted] controller with any other information requested by [redacted]

8.5 The [redacted] shall only on the Data Controller's instructions and [redacted] Personal Data to any Data Subject or to any other party [redacted] by the Data Controller, or as required by [redacted] domestic law.

9. Personal Data Breach

9.1 The [redacted] shall [immediately] **OR** [within <<insert time limit (hours/days) (or the maximum permitted delay)] notify the Data Controller in writing if it becomes aware of a Personal Data Breach including, but not limited to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

9.2 When the [redacted] becomes aware of a Personal Data Breach, it shall provide information to the Data Controller in writing without undue delay.

- a) [redacted] Personal Data Breach including the category or categories of Personal Data involved, the number (approximate or exact) of Personal Data records involved, and the number (approximate or exact, if known) of Data Subjects involved;
- b) [redacted] causes of the Personal Data Breach; and
- c) [redacted] measures it has taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its adverse effects.

9.3 In the event of a Personal Data Breach as described above, the Parties shall cooperate to investigate it. The Data Processor shall provide the Data Controller including, but not limited to:

- a) [redacted] controller with its investigation of the Personal Data Breach;
- b) [redacted] granting the Data Controller with access to any relevant data, information, systems, and personnel (including, if applicable, those involved in the Personal Data Breach);
- c) [redacted] records, logs, files, reports, and similar as requested by the Data Controller or as otherwise required by applicable legislation; and
- d) [redacted] reasonable steps to mitigate the effects of the Personal Data Breach and to minimise any damage caused by it.

9.4 The [redacted] shall use all reasonable endeavours to restore any Personal Data that has been lost, damaged, corrupted, or otherwise rendered unusable following a Personal Data Breach as soon as possible after becoming aware of the breach.

9.5 The [redacted] shall not inform any third party of any Personal Data Breach without the express written consent of the Data Controller, except to do so by domestic law.

9.6 The [redacted] will have the sole right to determine whether or not to notify the Information Commissioner, law enforcement agencies, the regulators of the Personal Data Breach as required by applicable regulations, or at the Data Controller's discretion of such notification.

9.7 The [REDACTED] have the sole right to determine whether or not to offer [REDACTED] subjects affected by the Personal Data Breach, including [REDACTED] of such remedy.

9.8 Subject to the provisions of Clause 16, the Data Processor shall bear all reasonable costs and expenses incurred by it and shall reimburse the Data Controller for the costs and expenses incurred by the Data Controller in connection with the Personal Data Breach, including the exercise of any of its obligations by the Data Controller under the applicable law, unless the Personal Data Breach resulted from the Data Processor's written instructions, negligence, breach of this Agreement or the Data Processor's omission of the Data controller, in which case the Data Processor shall bear and shall reimburse the Data Processor with such costs and expenses incurred by it.

10. Cross-Border Data

10.1 The [redacted] (and any subcontractor appointed by it) shall not process or transfer Personal Data outside of the EEA without the prior written consent of the Data Controller.

10.2 In the [REDACTED] controller consents to such a transfer or processing, the [REDACTED] only process (or permit the processing) of the Personal Data in the EEA if one or more of the following conditions are satisfied:

a) **P**rocessing the Personal Data in a territory that is regulated under the Data Protection Legislation provides adequate protection for the privacy rights of [territory] **OR** [territories] subject to such a finding shall be 4;

b) [REDACTED] participates in a valid cross-border transfer of personal data in accordance with the Data Protection Legislation under which the [REDACTED] (as the Data Controller, where appropriate) can demonstrate that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals in the UK in accordance with Article 46 of the UK GDPR. The transfer mechanism to be used is identified in Schedule 4. The Data Processor shall notify the Data Controller of any changes thereto; or

c) [REDACTED] Personal Data otherwise complies with the Data for the reasons set out in Schedule 4.

10.3 In the event of a transfer of Personal Data between the Data Controller and the Data Processor, the Data Controller requires the execution of Standard Contractual Clauses approved by the European Commission with the Data Protection Legislation (that is, where the Data Controller is transferring the Personal Data to the Data Processor, which is established in a country not within the EEA), the Parties shall complete all relevant details of the Standard Contractual Clauses set out in Schedule 5, execute the necessary legal actions and all other actions required to legitimise the transfer of the Personal Data.

- 10.4 [In the event that the Data Controller consents to the Data Processor appointing a subcontractor in accordance with the provisions of Clause 11, and the subcontractor is located outside of the EEA, the Data Controller hereby authorises the Data Processor to enter into Standard Contractual Clauses (SCCs) in Schedule 5, with the subcontractor in the Data Controller's name on the Data Controller's behalf. The Data Processor shall ensure that the subcontractor complies with the Standard Contractual Clauses available to the Data Controller.]
11. **Appointment of Subcontractors**
- 11.1 The Data Processor shall not subcontract any of its obligations or rights under this Agreement without the prior written consent of the Data Controller [(such consent may be withheld)].
- 11.2 In the event that the Data Processor appoints a subcontractor to process any of the Personal Data on its behalf, the Data Processor shall:
- enter into a written agreement with each subcontractor, which shall impose upon the subcontractor the same obligations, on substantially the same terms, as are imposed upon the Data Processor by this Agreement, with regard to technical and organisational measures required to comply with the Data Protection Regulations; and shall permit both the Data Processor and the Data Controller to audit the subcontractor's compliance with those obligations, and which shall terminate the subcontractor's appointment of this Agreement for any reason;
 - on the request of the Data Controller, provide copies of such agreement, and, if applicable, the relevant parts thereof;
 - ensure that the subcontractors comply fully with their obligations under the Agreement and under the Data Protection Regulations;
 - ensure that the subcontractors do not transfer all Personal Data transferred to subcontractors.
- 11.3 In the event that a subcontractor fails to meet its data protection obligations, the Data Processor shall remain fully liable to the Data Controller for the full compliance of the subcontractor with its data protection obligations.
- 11.4 The Data Processor shall be deemed to legally control any and all Personal Data processed by the subcontractors controlled practically by, or be in the possession of, and/or to which access is granted by it under this Clause 11.
12. **Return and Deletion of Personal Data**
- 12.1 The Data Processor shall, at the written request of the Data Controller (and at the request of the Data Controller, securely delete (or otherwise dispose of) the Personal Data in the format(s) reasonably requested by the Data Controller within a reasonable time after the earlier of
- the termination of the Services; or]
 - the termination of the Service Agreement, for any reason; or]

S

A

M

P

L

E

b) The retention of Personal Data by the Data Processor is no longer necessary for the performance of the Data Processor's obligations under the Agreement AND/OR [the Service Agreement].

12.2 Subject to Clause 8 [and 12.4], the Data Processor shall not retain all or any part of the Personal Data after deleting (or otherwise disposing of) or returning it to the Data Controller. 12.1.

12.3 If the Data Processor is required to retain copies of all or any part of the Personal Data by a law enforcement, government, or other regulatory body, it shall notify the Data Controller of such requirement(s) in writing, including the identity of the Data Controller, the Personal Data that it is required to retain, the legal basis for the requirement, the duration of the retention, and when the retained copies shall be deleted (or otherwise disposed of) once it is no longer required to retain them.

12.4 [The Data Processor shall retain one copy of the Personal Data for up to <<insert period>> purpose(s)>> only.]

12.5 Upon receipt of a request from the Data Controller, the Data Processor shall certify the deletion (or disposal) of the Personal Data, the Data Processor shall provide the same in writing to the Data Controller within <<insert period>> of deletion (or disposal).

12.6 [All Personal Data deleted or disposed of under this Agreement shall be done using the following method(s): <<insert description of method(s)>>]

13. Information

13.1 The Data Processor shall make available to the Data Controller any and all information, including but not limited to, reasonably required and necessary to demonstrate the Data Processor's compliance with the Data Protection Legislation and this Agreement.

13.2 [The Data Processor shall maintain complete, accurate, and up-to-date written records of all activities carried out by the Data Processor on behalf of the Data Controller, which shall include:

a) Details of the Data Processor and the Data Controller, including, where applicable, each Party's representative and data protection officer;

b) Details of the processing carried out by the Data Processor;

c) Details of transfers of personal data to a third country and the safeguards; and

d) Details of the technical and organisational security measures referred to in Clause 7.]

14. Audits

14.1 The Data Controller shall have the right to audit or request the Data Processor to allow the Data Controller or a third-party auditor to audit the Data Processor's compliance with this Agreement and with the Data Protection Legislation on [at least <<insert period>> days'] OR [reasonable grounds] to allow the Data Controller or a third-party auditor to audit the Data Processor's compliance with this Agreement and with the Data Protection Legislation.

14.2 The Data Processor shall provide all necessary assistance [(at its own cost)] OR [at the Data Controller's cost] in the conduct of such audits including, but not limited to, providing access to all relevant data and documentation.

not li

a) [Physical and remote) to, and copies of, all [Records of processing] information kept by the Data Processor;

b) [Employees who are to access and/or process any of the Personal Data], including, where reasonably necessary, arranging for the Data Controller and such employees; and

c) [Protection of all [Records,] infrastructure, equipment, and systems used to store and/or process the Personal Data]

14.3 The Data Controller shall give notice under sub-Clause 14.1 if it has reason to believe that the Data Processor has failed to comply with its obligations under this Agreement or under the Data Protection Legislation, or if it has reason to believe that a Personal Data Breach is taking place.

14.4 The Data Controller shall inform the Data Controller [immediately] OR [promptly] of any instructions given by the Data Controller or any third-party which the Data Controller do not comply with the

15. Warranties

15.1 The Data Controller warrants and represents that the Personal Data [the Data Controller] OR [the Service Agreement] and this Agreement shall comply with the Data Protection Legislation in all respects including its collection, holding, and processing.

15.2 The Data Controller warrants and represents that:

a) [All] Personal Data shall be processed by the Data Processor (and by any sub-processors appointed under Clause 11) in compliance with the Data Protection Legislation and any and all other relevant laws, regulations, orders, standards, and other similar

b) [The Data Controller] does not believe that the Data Protection Legislation in any way prevents it from complying with its obligations [pertaining to the Data Controller] OR [under the Service Agreement]; and

c) [The Data Controller] has implemented appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing or disclosure, accidental loss, destruction, or damage, as set out in Schedule 3.

16. Liability and

16.1 The Data Controller shall be liable for, and shall indemnify (and keep the Data Processor in respect of, any and all actions, claims, losses, expenses (including reasonable legal fees on a solicitor and client basis), or demands, suffered by the Data Processor, or agreed to be paid by, the Data Processor [and any sub-processors appointed by the Data Processor under Clause 11] arising from or in connection with:

- a) by the Data Controller with the Data Protection
 - b) processing carried out by the Data Processor [or appointed by the Data Processor under Clause 11] in accordance with instructions given by the Data Controller to the extent that the instructions are in compliance with the Data Protection Legislation; or
 - c) the Data Processor of its obligations or warranties under the same is or are contributed to by any non-controller with the Data Protection Legislation or its breach
- 16.2 The Data Processor shall not be liable for, and shall indemnify (and keep the Data Controller in respect of, any and all actions, claims, losses, expenses (including reasonable legal costs on a solicitor and client basis), or demands, suffered or incurred by, or agreed to be paid by, the Data Controller in connection with:
- a) processing carried out by the Data Processor [or any subcontractor appointed by the Data Processor under Clause 11] with the Data Protection Legislation; or
 - b) processing carried out by the Data Processor [or appointed by the Data Processor under Clause 11] in accordance with instructions given by the Data Controller to the extent that the instructions are in compliance with the Data Protection Legislation; or
 - c) the Data Processor of its obligations or warranties under the same is or are contributed to by any non-controller with the Data Protection Legislation or its breach
- 16.3 The Data Processor shall not be entitled to claim back from the Data Controller under Clause 16.2 or on any other basis any sums paid in connection with the Data Controller in respect of any damage to the extent that the Data Processor is able to indemnify the Data Processor under sub-Clause 16.2
- 16.4 Nothing in this Clause 16) shall relieve either Party from, and in particular, this Clause 16) shall relieve neither Party from, the effect, the liability of either Party to any Data Protection Legislation. Furthermore, the Data Processor hereby acknowledges that it remains subject to the authority of the Information Commissioner and shall operate fully therewith, as required, and that the Data Processor shall remain subject to the fines, penalties, and obligations as a data processor under the Data Protection Legislation. Furthermore, the Data Processor shall remain subject to the fines, penalties, and obligations as a data processor under the Data Protection Legislation.
- 16.5 Subject to the provisions of this Clause 16, nothing in this Clause 16 shall be deemed to be affected by any other provision(s) of this Agreement.
- 16.6 [Any provisions of the Service Agreement shall not apply to any provisions set out in this Agreement.]

17. **Term and Termination**

17.1 This Agreement shall be in force on <<insert commencement date>> and shall continue in force for a period of <<insert period>> or, if longer of:

- a) the period of <<insert period>> for the provision of the services, as set out in Schedule 1; or]
- a) the period for which the Service Agreement remains in effect; or]
- b) the period for which the Data Processor has any of the Personal Data in its possession or control.

17.2 Any provision of this Agreement which, expressly or by implication, is to come into force on or after [its termination or expiry] **OR** [the termination of the Service Agreement] shall remain in full force and effect.

17.3 In the event that the provisions of the Data Protection Legislation necessitate the renegotiation of this Agreement, either Party may require such renegotiation.

18. **Notices**

18.1 All notices in connection with this Agreement shall be in writing.

18.2 All notices to the Data Controller under or in connection with this Agreement shall be addressed to: <<insert name, position (e.g. data controller) and contact details>>.

18.3 All notices to the Data Processor under or in connection with this Agreement shall be addressed to: <<insert name, position (e.g. data processor) and contact details>>.

18.4 Notices shall have been duly given:

- a) if delivered by courier or other messenger (including electronic mail) during normal business hours of the recipient; or
- b) if sent by post, facsimile or e-mail [and a successful return receipt is generated]; or
- c) if sent by post, the day following mailing, if mailed by national registered post, pre-paid.

In each case, the notice shall be addressed as indicated above.

19. **Law and Jurisdiction**

19.1 This Agreement, and any non-contractual matters and obligations arising therefrom (whether or not in connection with the Agreement), shall be governed by, and construed in accordance with, the law of England and Wales.

19.2 Any proceedings or claim between the Parties relating to this Agreement, or any non-contractual matters and obligations arising therefrom (whether or not in connection with the Agreement), shall fall within the jurisdiction of the courts of England and Wales.

SIGNED for and on behalf of the Controller by:
<<Name and Title of the Data Controller>>

Authorised Signatory

Date: _____

SIGNED for and on behalf of the Processor by:
<<Name and Title of the Data Processor>>

Authorised Signatory

Date: _____

S

SCHEDULE 1

Services

<<Insert a detailed description of the services provided by the Data Processor (under the Service Agreement, if applicable).

A

M

P

L

E

S

SCHEDULE 2

Personal Data

Type of Personal Data	Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing	Duration of Processing

A

M

P

L

F

Technical and Organisational Measures**Technical and Organisational Measures**

The following measures shall be implemented in Clause 1.1

organisational data protection measures referred to in Clause 1.1

1. The Data Processor shall, in respect of all Personal Data it receives from the Data Controller, it maintains security measures to a standard appropriate to the risk of the following:
 - 1.1 the loss of the Personal Data from unlawful or unauthorised processing or destruction of the Personal Data; and
 - 1.2 the loss of the Personal Data.
2. In particular, the Data Processor shall:
 - 2.1 have in place, a security policy which:
 - a) is based on a risk assessment;
 - b) is subject to regular review for implementing the policy to a specific level (the Data Processor's data protection officer)] or
 - c) is approved by the Data Controller on or before the commencement of the processing;
 - d) is communicated to relevant staff; and
 - e) is subject to regular review for feedback and review.
 - 2.2 ensure that security safeguards and virus protection are in place to protect the Personal Data from malware which is used in processing the Personal Data in line with best industry practice;
 - 2.3 ensure that security safeguards are in place for the software used in the processing of the Personal Data, including but not limited to, the installation of all security updates;
 - 2.4 prevent the loss of the Personal Data;
 - 2.5 protect the Personal Data using <<insert type of encryption>> encryption;
 - 2.6 protect the Personal Data using pseudonymisation, where it is practical to do so;
 - 2.7 ensure that the Personal Data conforms with best industry practice such that Personal Data is recorded (including paper records and electronic records) are stored in secure locations and the Personal Data is strictly monitored and controlled;
 - 2.8 have in place for the transfer of Personal Data whether in physical form (e.g. by using couriers rather than post) or electronic form (e.g. <<insert type of encryption>> encryption);
 - 2.9 pass on to the Data Controller the details of the devices on which Personal Data is stored and ensure that the passwords are secure (<<describe requirements, e.g. minimum length, use of special characters etc.>>), and that passwords are not shared with third parties in any circumstances;

- 2.10 [not a laptop] Personal Data on any mobile devices such as mobile devices are kept on its premises at all times;]
- 2.11 take measures to ensure the reliability of personnel who have access to the Data Controller's premises;
- 2.12 ensure that all personnel who are to access and/or process any of the Personal Data receive adequate training on the Data Protection Legislation, the Data Controller's policies under it, their obligations under it, and its application with particular regard to the processing of the Personal Data in accordance with the Data Protection Legislation;
- 2.13 have procedures in place for detecting and dealing with breaches of security (including the destruction of Personal Data) including:
- 2.13.1 identifying which individuals have worked with specific Personal Data;
- 2.13.2 a procedure in place for investigating and remedying breaches of the Data Protection Legislation; and
- 2.13.3 notifying the Data Controller as soon as any such security breach has occurred;
- 2.14 have procedures in place for backing up all electronic Personal Data and storing them securely, separate from originals;
- 2.15 have procedures in place for the disposal of unwanted Personal Data including for the disposal of redundant equipment; [and]
- 2.16 [where applicable, details as required]; and]
- 2.17 adopt appropriate operational, and technological processes and procedures to comply with the requirements of ISO/IEC 27001 in relation to the Services provided to the Data Controller.

S

SCHEDULE 4

Legal Basis for Processing Personal Data Outside the EEA

The Data Processor is processing the Personal Data outside of the EEA in order to comply with the following restrictions is as follows:

[The Data Processor is processing the Personal Data outside of the EEA with a current determination of adequacy: <<insert country>>.]

OR

[Binding Corporate

OR

[Standard Contractual Clauses between the Data Controller as the “data exporter” and the Data Processor as the “data importer”.]

OR

[Standard Contractual Clauses between the Data Processor as the “data exporter” on behalf of the Data Controller as the “data importer” or the Data Processor’s affiliate or subcontractor as the “data exporter” and the Data Controller as the “data importer”.]

OR

[<<insert alternative legal basis for processing the Personal Data in detail>>.]

A

M

P

L

E

S

A

M

P

L

E