DATA PROCESSING AGREEMENT

Note

When you operate your own Parent account, you are the Data Controller and peopleMaps is the Data processor. When you create a Child Account you are considered a **Data Sub Processor,** as you have the facility to create Child accounts via your PeopleMaps Control Room and access the data held on those accounts. These Child accounts may be used by people or organisations other than your own. This means they may be gathering personal data from individuals and you will be able to access that data. Therefore, you and they are subject to comply with GDPR data protection laws.

If you create a Child account that is used by a third party, they are the **Data Controller**, PeopleMaps is the **Data Processor,** as the data is held on the PeopleMaps server and you are effectively the **Data Sub Processor**.

This agreement is designed to ensure that you, your clients and PeopleMaps all comply with GDPR data protection laws.

THIS AGREEMENT i**BETWEEN:**

(1) PeopleMaps Limited a limited company registered in England under company number 03904001 , whose registered address is Carrwood Park, Selby Road, Leeds, LS15 4LG, and whose main trading address is Regent Court, 70 West Regent Street, Glasgow, G2 2QZ. ("**PeopleMaps is both the Data Controller and Data Processor and for the purposes of this agreement will be referred to as the Data Controller"**) and

(2) The account holder who ticked the consent box, hereafter referred to as the **Data Sub Processor**

This agreement commences as soon as the account holder ticked the consent box and will run for as long as the Data Sub Processor has access to their PeopleMaps Account.

WHEREAS:

(1) Under a written agreement between the Data Controller and the Data Sub Processor dated 5th June 2018 ("the Service Agreement") the Data Sub Processor provides to the Data Controller the Services described in Schedule 1.

(2) The provision of the Services by the Data Sub Processor involves it in processing the Personal Data described in Schedule 2 on behalf of the Data Controller.

(3) Under EU Regulation 2016/679 General Data Protection Regulation ("the GDPR") (Article 28, paragraph 3), the Data Controller is required to put in place an agreement in writing between the Data Controller and any organisation which processes personal data on its behalf governing the processing of that data.

(4) The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of the GDPR in relation to all processing of the Personal Data by the

Data Sub Processor for the Data Controller.

(5) The terms of this Agreement are to apply to all processing of Personal Data carried out for the Data Controller by the Data Sub Processor and to all Personal Data held by the Data Sub Processor in relation to all such processing.

IT IS AGREED as follows:

1. **Definitions and Interpretation**

1.1 In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Data Controller", "Data Processor", "processing", "data subject", and "personal data breach"	shall have the meanings given to the terms "controller", "processor", "processing", "data subject", and "personal data breach" respectively in Article 4 of the GDPR;
"Data Protection Legislation"	means all applicable privacy and data protection laws including the GDPR and any applicable national implementing laws, regulations, and secondary legislation in England and Wales, as amended, replaced, or updated from time to time, including the Privacy and Electronic Communications Directive 2002 (2002/58/EC) and the Privacy and Electronic Communications (EC Directive) Regulations 2003;
"ICO"	means the UK's supervisory authority, the Information Commissioner's Office;
"Personal Data"	means all such "personal data", as defined in Article 4 of the GDPR, as is, or is to be, processed by the Data Sub Processor on behalf of the Data Controller, as described in Schedule 2;
"Services"	means those services described in Schedule 1 which are provided by the Data Sub Processor to the Data Controller and which the Data Controller uses for the purpose**[s]** described in Schedule 1;
"Standard Contractual Clauses"	means the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to data sub processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU, a complete copy of which is included in Schedule 4;
"Sub-Processor"	means a sub-contractor appointed by the Data Controller to process the Personal Data; and

"Sub-Processing Agreement"	means an agreement between the Data Processor and a Sub-Processor governing the Personal Data processing carried out by the Sub-Processor, as described in Clause 10.
"Term"	means the term of this Agreement, as set out in sub-Clause 14.1.

1.2 Unless the context otherwise requires, each reference in this Agreement to:

2.a.1 "writing", and any cognate expression, includes a reference to any communication affected by electronic or facsimile transmission or similar means;

2.a.2 a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

2.a.3 "this Agreement" is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;

2.a.4 a Schedule is a schedule to this Agreement; and

2.a.5 a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule.

2.a.6 a "Party" or the "Parties" refer to the parties to this Agreement.

1.3 The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.

1.4 Words imparting the singular number shall include the plural and vice versa.

1.5 References to any gender shall include the other gender.

1.6 References to persons shall include corporations.

2. Scope and Application of this Agreement

1.1 The provisions of this Agreement shall apply to the processing of the Personal Data described in Schedule 2, carried out for the Data Controller by the Data Sub Processor, and to all Personal Data held by the Data Sub Processor in relation to all such processing whether such Personal Data is held at the date of this Agreement or received afterwards.

1.2 In the event of any conflict or ambiguity, the following shall apply:

2.a.1 Where there is any conflict or ambiguity between a provision contained in the body of this Agreement and any provision contained in a Schedule to this Agreement, the provision in the body of this Agreement shall prevail;

2.a.2 Where there is any conflict or ambiguity between the terms of any invoice or other document annexed to this Agreement and any provision contained in a Schedule to this Agreement, the provision contained in the Schedule shall prevail;

2.a.3 Where there is any conflict or ambiguity between a provision of this Agreement and a provision of the Service Agreement, the provision in this Agreement shall prevail; and

2.a.4 Where there is any conflict or ambiguity between a provision of this Agreement and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses shall prevail.

3. **Provision of the Services and Processing Personal Data**

1.1 The Data Sub Processor is only to carry out the Services, and only to process the Personal Data received from the Data Controller:

1.a.1 for the purposes of those Services and not for any other purpose;

1.a.2 to the extent and in such a manner as is necessary for those purposes; and

1.a.3 strictly in accordance with the express written authorisation and instructions of the Data Controller (which may be specific instructions or instructions of a general nature or as otherwise notified by the Data Controller to the Data Sub Processor).

1.2 The Data Controller shall retain control of the Personal Data and shall remain responsible for its compliance obligations under the Data Protection Legislation including, but not limited to, providing the required notices and obtaining any required consents, and for any and all processing instructions it gives to the Data Sub Processor.

4. **Data Protection Compliance**

1.1 All instructions given by the Data Controller to the Data Sub Processor shall be made in writing and shall at all times be in compliance with the Data Protection Legislation and other applicable laws. The Data Sub Processor shall act only on such written instructions from the Data Controller unless the Data Sub Processor is required by law to do otherwise.

1.2 The Data Sub Processor shall promptly comply with any request from the Data Controller requiring the Data Sub Processor to amend, transfer, delete, or otherwise dispose of the Personal Data, or to cease, mitigate, or remedy any authorised processing.

1.3 The Data Sub Processor shall transfer all Personal Data to the Data Controller on the Data Controller's request in the formats, at the times, and in compliance with the Data Controller's written instructions.

1.4 Both Parties shall comply at all times with the Data Protection Legislation and shall not perform their obligations under this Agreement or any other agreement or arrangement between themselves in such way as to cause either Party to breach any of its applicable obligations under the Data Protection Legislation.

1.5 The Data Controller hereby warrants, represents, and undertakes that the Personal Data and its use with respect to the Service Agreement and this Agreement shall comply with the Data Protection Legislation in all respects

including, but not limited to, its collection, holding, and processing.

1.6 The Data Sub Processor hereby warrants, represents, and undertakes that:

6.a.1 all of its personnel (including, but not limited to, its employees, agents, and sub-contractors) that will access the Personal Data are reliable, trustworthy, and have been suitably trained on the Data Protection Legislation as it relates to this Agreement;

6.a.2 the Personal Data shall be processed by the Data Sub Processor (and any Sub-Processors it may appoint) in compliance with the Data Protection Legislation and any and all other relevant laws, enactments, regulations, orders, standards, and other similar instruments;

6.a.3 it has no reason to believe that the Data Protection Legislation in any way prevents it from complying with its obligations under the Service Agreement; and

6.a.4 it will implement appropriate technical and organisational measures to prevent the unauthorised and/or unlawful processing of the Personal Data and/or the accidental loss of, destruction of, or damage to the Personal Data, ensuring levels of security that are appropriate and proportionate to the harm that may result from such processing, loss, or damage, to the nature of the Personal Data, and that are appropriate to ensure compliance with the Data Protection Legislation and with its own security policy including, but not limited to, the security measures required under Clause 9.

1.7 The Data Sub Processor agrees to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with any and all applicable legislation from time to time in force (including, but not limited to, the Data Protection Legislation) and any best practice guidance issued by the ICO and/or any other applicable supervisory authority.

1.8 The Data Sub Processor shall provide all reasonable assistance to the Data Controller in complying with its obligations under the GDPR with respect to the security of processing, the notification of personal data breaches, the conduct of data protection impact assessments, and in dealings with the ICO and/or any other applicable supervisory authority.

1.9 When processing the Personal Data on behalf of the Data Controller, the Data Sub Processor shall:

9.a.1 not transfer any of the Personal Data to any third party without the written consent of the Data Controller and, in the event of such consent, the Personal Data shall be transferred strictly subject to the terms of a suitable agreement, as set out in Clause 10;

9.a.2 not transfer any of the Personal Data to any territory outside of the European Economic Area (“EEA”) without the written consent of the Data Controller and, in the event of such consent, only if the applicable conditions set out in Clause 11 are satisfied;

9.a.3 process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Data Controller or as may be required by law (in which case, the Data Sub

Processor shall inform the Data Controller of the legal requirement in question before processing the Personal Data for that purpose unless prohibited from doing so by law);

9.a.4 implement appropriate technical and organisational measures, as described in Clause 9 and Schedule 3, and take all steps necessary to protect the Personal Data;

9.a.5 if so requested by the Data Controller (and within the timescales required by the Data Controller) supply further details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access;

9.a.6 keep detailed records of all processing activities carried out on the Personal Data in accordance with the requirements of the Data Protection Legislation and as set out in Clause 16;

9.a.7 make available to the Data Controller any and all such information as is reasonably required and necessary to demonstrate the Data Sub Processor's compliance with the Data Protection Legislation;

9.a.8 on reasonable prior notice, submit to audits and inspections and provide the Data Controller with any information reasonably required in order to assess and verify compliance with the provisions of this Agreement and both Parties' compliance with the requirements of the GDPR, as set out in Clause 17. The requirement to give notice will not apply if the Data Controller has reason to believe that a personal data breach has taken place or is taking place or that the Data Sub Processor is in breach of any of its obligations under this Agreement or under the Data Protection Legislation;

9.a.9 inform the Data Controller immediately if it is asked to do anything that infringes the Data Protection Legislation or any other applicable data protection legislation; and

9.a.10 inform the Data Controller promptly if any changes to the Data Protection Legislation may adversely affect its performance of its obligations under the Service Agreement.

5. Data Subject Rights, Complaints, and Personal Data Breaches

1.1 The Data Sub Processor shall assist the Data Controller in complying with its obligations under the Data Protection Legislation. In particular, the provisions of this Clause 5 shall apply to:

1.a.1 the exercise by data subjects of their rights (including subject access rights, the rights to rectification and erasure of personal data, the rights to object to processing, restrict processing, and rights relating to automated processing), complaints, and personal data breaches; and

1.a.2 notices served on the Data Controller by the ICO or any other applicable supervisory authority under the Data Protection Legislation.

1.2 The Data Sub Processor shall notify the Data Controller immediately if it receives any complaint, notice, or other communication concerning the processing of the Personal Data (whether directly or indirectly) or either

Party's compliance with the Data Protection Legislation.

1.3 The Data Sub Processor shall notify the Data Controller without undue delay and, in any event, within 72, if it receives a data subject access request or a request from a data subject to exercise any of their other rights under the Data Protection Legislation.

1.4 The Data Sub Processor shall cooperate fully with the Data Controller and assist as required in relation to any complaint, notice, communication, or data subject request, including by:

4.a.1 providing the Data Controller with full details of the complaint, notice, communication, or request;

4.a.2 providing the necessary information and assistance in order to comply with the complaint, notice, communication, or request;

4.a.3 providing the Data Controller with any Personal Data it holds in relation to a data subject (within the timescales required by the Data Controller); and

4.a.4 providing the Data Controller with any other information requested by the Data Controller.

1.5 The Data Sub Processor shall promptly and without undue delay notify the Data Controller if any of the Personal Data is lost or destroyed, or becomes damaged, corrupted, or otherwise unusable. Any Personal Data so affected shall be restored by the Data Sub Processor at the Data Sub Processor's own cost.

1.6 The Data Sub Processor shall notify the Data Controller immediately if it becomes aware of any accidental, unauthorised, or unlawful processing of the Personal Data, or of any personal data breach. The following information shall also be provided to the Data Controller without undue delay:

6.a.1 a full description of the nature of the event, including the category or categories of Personal Data concerned, the category or categories of data subject concerned, and the approximate number of both Personal Data records and data subjects involved;

6.a.2 details of the likely consequences; and

6.a.3 details of the measures taken, or planned, to address the event, including those intended to mitigate possible adverse effects.

1.7 Immediately following any event under sub-Clause 5.6, the Data Controller and the Data Sub Processor shall jointly investigate that event. In particular, the Data Sub Processor shall cooperate fully with the Data Controller and assist as required, including by:

7.a.1 assisting with any investigation;

7.a.2 providing the Data Controller with access to any premises, facilities, and/or operations involved;

7.a.3 facilitating interviews with any of the Data Sub Processor's personnel, former personnel, and any other individuals involved;

7.a.4 providing or making available to the Data Controller any and all relevant records, logs, files, reports, and other documentation and

materials required to comply with the Data Protection Legislation or other such materials reasonably required by the Data Controller; and

7.a.5 taking all reasonable steps, promptly, to mitigate the effects of the event and to minimise any damage arising from it.

1.8 The Data Sub Processor shall not inform any third party of any Personal Data breach without the prior written consent of the Data Controller unless it is required to do so by law.

1.9 The Data Controller shall have the sole right to determine the following:

9.a.1 whether or not to notify Personal Data breaches to data subjects, the ICO or other applicable supervisory authorities, regulators, law enforcement agencies, or others, as required by law or at the Data Controller's discretion;

9.a.2 the content and means of delivery of any such notice under sub-Clause 5.9.1; and

9.a.3 whether or not to offer a remedy to affected data subjects and, where such a remedy is to be offered, the nature and extent thereof.

6. **Appointment of a Data Protection Officer**

1.1 The Data Controller has appointed a Data Protection Officer in accordance with Article 37 of the GDPR, whose details are as follows: Martin Gibbons martin@peoplemaps.co.uk

1.2 []

1.3 The Data Sub Processor has appointed a Data Protection Officer in accordance with Article 37 of the GDPR, whose details are displayed by logging in to your PeopleMaps Control Room as the parent account holder and going to **>>Settings >>My Account**. The main contact will be considered to be the Data Protection Officer. The

7. **Confidentiality**

1.1 The Data Sub Processor shall maintain the Personal Data in confidence, and in particular, unless the Data Controller has given written consent for the Data Sub Processor to do so, the Data Sub Processor shall not disclose any Personal Data supplied by the Data Controller to any third party. The Data Sub Processor shall not process or make any use of any Personal Data supplied to it by the Data Controller otherwise than in connection with the provision of the Services to the Data Controller.

1.2 If the Data Sub Processor is required by law, a court, regulator, the ICO, or any other applicable supervisory authority to disclose or process any of the Personal Data, the Data Sub Processor shall inform the Data Controller before making any such disclosure or carrying out any such processing, giving the Data Controller the opportunity to object to or challenge the requirement,

unless the Data Sub Processor is prohibited from doing so by law.

8. **Data** Sub **Processor's Personnel**

1.1 The Data Sub Processor shall ensure that all personnel who are to access and/or process any of the Personal Data:

1.a.1 are aware both of the Data Sub Processor's duties and obligations, and of their own individual duties and obligations under this Agreement and the Data Protection Legislation;

1.a.2 have been given suitable training on the Data Protection Legislation with respect to the handling of Personal Data and how the Data Protection Legislation applies to their particular duties; and

1.a.3 are contractually obliged to keep the Personal Data confidential.

1.2 The Data Sub Processor shall take reasonable steps to ensure the reliability, integrity, and trustworthiness of all personnel who are to access and/or process any of the Personal Data

9. **Security**

The Data Sub Processor shall implement suitable technical and organisational security measures in order to protect the Personal Data against unauthorised or unlawful access, processing, disclosure, copying, alteration, storage, reproduction, display, or distribution; and against loss, destruction, or damage, whether accidental or otherwise. Such measures shall include, but not be limited to, those set out in Schedule 3. Such measures shall be fully documented in writing by the Data Sub Processor and be reviewed at least annually to ensure that they remain up-to-date, complete, and appropriate. The Data Sub Processor shall inform the Data Controller in advance of any changes to such measures.

10. **Appointment of Sub-Processors**

1.1 The Data Sub Processor **shall not** sub-contract any of its obligations or rights under this Agreement without the prior written consent of the Data Controller.

11. **Cross-Border Transfers of Personal Data**

1.1 The Data Sub Processor shall not transfer or otherwise process any of the Personal Data outside of the European Economic Area ("EEA") without the prior written consent of the Data Controller.

12. **Liability and Indemnity**

1.1 The Data Controller shall be liable for, and shall indemnify (and keep indemnified) the Data Sub Processor in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Data Sub

Processor arising directly or in connection with:

1.a.1 any non-compliance by the Data Controller with the Data Protection Legislation or other applicable legislation;

1.a.2 any Personal Data processing carried out by the Data Sub Processor in accordance with instructions given by the Data Controller that infringe the Data Protection Legislation or other applicable legislation; or

1.a.3 any breach by the Data Controller of its obligations under this Agreement,

except to the extent that the Data Sub-Processor is liable under sub-Clause 12.2.

1.2 The Data Sub Processor shall be liable for, and shall indemnify (and keep indemnified) the Data Controller in respect of any and all action, proceeding, liability, cost, claim, loss, expense (including reasonable legal fees and payments on a solicitor and client basis), or demand suffered or incurred by, awarded against, or agreed to be paid by, the Data Controller arising directly or in connection with:

2.a.1 any non-compliance by the Data Sub Processor with the Data Protection Legislation or other applicable legislation;

2.a.2 any failure by the Data Sub Processor or any of its employees, agents, or sub-contractors to comply with any of its obligations under this Agreement; or

2.a.3 the Data Sub Processor's Personal Data processing activities that are subject to this Agreement:

a.3.a.1 only to the extent that the same results from the Data Sub Processor's breach of this Agreement; and

a.3.a.2 not to the extent that the same is or are contributed to by any breach of this Agreement by the Data Controller.

1.3 The Data Controller shall not be entitled to claim back from the Data Sub-Processor any sums paid in compensation by the Data Controller in respect of any damage to the extent that the Data Controller is liable to indemnify the Data Sub-Processor under sub-Clause 12.1.

1.4 Nothing in this Agreement (and in particular, this Clause 12) shall relieve either Party of, or otherwise affect, the liability of either Party to any data subject, or for any other breach of that Party's direct obligations under the Data Protection Legislation. Furthermore, the Data Sub Processor hereby acknowledges that it shall remain subject to the authority of the ICO and any other applicable supervisory authorities, and shall co-operate fully therewith, as required, and that failure to comply with its obligations as a data sub processor under the Data Protection Legislation may render it subject to the fines, penalties, and compensation requirements set out in the Data Protection Legislation.

1.5 No limitation of liability set out in the Service Agreement shall apply to the indemnity provisions or reimbursement obligations of this Agreement.

13. **Intellectual Property Rights**

All copyright, database rights, and other intellectual property rights subsisting in the Personal Data (including but not limited to any updates, amendments, or adaptations to the Personal Data made by either the Data Controller or the Data Sub Processor) shall belong to the Data Controller or to any other applicable third party from whom the Data Controller has obtained the Personal Data under licence (including, but not limited to, data subjects, where applicable). The Data Sub Processor is licensed to use such Personal Data under such rights only for the purposes of the Services, and in accordance with this Agreement.

14. **Term and Termination**

1.1 This Agreement shall remain in full force and effect:

1.a.1 for as long as the Service Agreement remains in effect; or

1.a.2 for as long as the Data Sub Processor retains any Personal Data relating to the Service Agreement in its possession or control,

whichever period is longer.

1.2 Where any provision of this Agreement, whether expressly or by implication, either comes into force, or continues in force on or after the termination of the Service Agreement in order to protect the Personal Data, that provision shall remain in full force and effect.

1.3 Any failure by the Data Sub Processor to comply with the terms of this Agreement shall be deemed to be a material breach of the Service Agreement. In the event of such a breach, the Data Controller shall have the right to terminate the Service Agreement, such termination to be effective immediately on written notice to the Data Sub Processor, without further liability or obligation.

1.4 If any change to the Data Protection Legislation prevents either Party from fulfilling any of its obligations under the Service Agreement, the processing of the Personal Data shall be suspended until such processing can be made to comply with the Data Protection Legislation, as amended. If such processing cannot be made to comply, the Parties may terminate the Service Agreement on written notice to one another.

15. **Deletion and/or Disposal of Personal Data**

1.1 []

1.2 If the Data Sub Processor is required by law, government, or other regulatory body to retain any documents or materials that the Data Sub Processor would otherwise be required to return, delete, or otherwise dispose of under this Agreement, the Data Sub Processor shall notify the Data Controller in writing of the requirement. Such notice shall give details of all documents or materials that the Data Sub Processor is required to retain, the legal basis for that retention, and the timeline for deletion and/or disposal at the end of the retention period.

1.3 All Personal Data to be deleted or disposed of under this Agreement shall be

deleted or disposed of using the following method(s): ZERO WRITE..

16. **Record Keeping**

1.1 The Data Sub Processor shall keep suitably detailed, accurate, and up-to-date written records of any and all processing of the Personal Data carried out for the Data Controller. Such records shall include, but not be limited to, access, control, security, sub-contractors, affiliates, the purpose(s) for which the Personal Data is processed, the category or categories of processing, transfers of the Personal Data to non-EEA territories and related safeguards, and details of the technical and organisational security measures referred to in Clause 9.

1.2 The Data Sub Processor shall ensure that such records are sufficient to enable the Data Controller to verify the Data Sub Processor's compliance with the provisions of this Agreement and with the Data Protection Legislation. The Data Sub Processor shall provide the Data Controller with copies of such records on request.

1.3 The Data Sub Processor shall review the information contained in the Schedules to this Agreement at least every six months in order to ensure that it remains accurate and up-to-date with current practices.

17. **Auditing**

1.1 The Data Sub Processor shall permit the Data Controller and any third-party representatives that the Data Controller may from time to time appoint to audit its compliance with its obligations under this Agreement, on reasonable prior notice during the Term of this Agreement.

1.2 The Data Sub Processor shall provide to the Data Controller and any third-party representatives all necessary assistance in conducting such audits including, but not limited to:

2.a.1 physical and electronic access to, and copies of, records kept under Clause 16 and any other information pertaining to the processing of the Personal Data;

2.a.2 access to (and meetings with) any of the Data Sub Processor's personnel that are reasonably necessary to audit the Data Sub Processor's compliance with this Agreement; and

2.a.3 inspection of any and all infrastructure, systems, facilities, equipment, electronic data, and software used for the storage, transfer, and processing of the Personal Data.

1.3 Prior to commencing the processing of the Personal Data and thereafter on a annual basis, the Data Sub Processor shall:

3.a.1 carry out an information security audit in order to identify any security deficiencies;

3.a.2 produce a written report of its audit which shall include plans to remedy any such deficiencies;

3.a.3 provide the Data Controller with a copy of the report; and

3.a.4 remedy any defects identified in its audit within 30 days

1.4 The notice requirement set out in sub-Clause 17.1 shall not apply if the Data Controller has reason to believe that a personal data breach has taken place or is taking place, or that the Data Sub Processor is in breach of any of its obligations under this Agreement or the Data Protection Legislation.

1.5 In the event of a personal data breach (including if the Data Sub Processor becomes aware of any breach of its obligations under this Agreement or the Data Protection Legislation), the Data Processor shall:

5.a.1 conduct its own audit to determine the cause of said breach within 72 hours of the triggering event;

5.a.2 produce a written report of its audit which shall include plans to remedy any deficiencies identified thereby;

5.a.3 provide the Data Controller with a copy of the report; and

5.a.4 remedy any defects identified in its audit within 30 days.

18. **[]**

19. **Law and Jurisdiction**

1.1 This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.

1.2 Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of Scotland.

SCHEDULE 1

Services

Data Sub Processor provides first line customer support to clients it has created Child Accounts for and as such has access to Child Account data.

All data is held and managed by the Peoplemaps System which is Software as a Service. PeopleMaps remains the Data Processor.

SCHEDULE 2

Personal Data

Type of Personal Data	Category of Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing
Typical data held is first name, last name, email, telephone, preferred pronoun, gender, postal address. However, Child Account Holders may customise their registration form and collect additional data. This data will also be treated properly as per the GDPR data protection laws.	**registration details**	first line support	support

SCHEDULE 3

Technical and Organisational Data Protection Measures

The following are the technical and organisational data protection measures referred to in Clause 9:

1. The Data Sub Processor shall ensure that, in respect of all Personal Data it receives from or processes on behalf of the Data Controller, it maintains security measures to a standard appropriate to:

   1.1 the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Personal Data; and

   1.2 the nature of the Personal Data.

2. In particular, the Data Sub Processor shall:

   1.1 have in place, and comply with, a security policy which:

      1.a.1 defines security needs based on a risk assessment;

      1.a.2 allocates responsibility for implementing the policy to a specific individual (such as the Data Sub Processor's Data Protection Officer)**]**or personnel;

      1.a.3 is provided to the Data Controller on or before the commencement of this Agreement;

      1.a.4 is disseminated to all relevant staff; and

      1.a.5 provides a mechanism for feedback and review.

   1.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Personal Data in accordance with best industry practice;

   1.3 ensure that the effectiveness of all measures detailed in this Agreement and in any specific security policy are regularly tested, assessed, and evaluated;

   1.4 prevent unauthorised access to the Personal Data;

   1.5 protect the Personal Data using pseudonymisation, where it is practical to do so;

   1.6 implement such measures as are necessary to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services used to process Personal Data;

   1.7 ensure that its storage of Personal Data conforms with best industry practice such that the media on which Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Personal Data is strictly monitored and controlled;

   1.8 have secure methods in place for the transfer of Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using encryption);

1.9 password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure and that passwords are not shared under any circumstances;

1.10 not allow the storage of the Personal Data on any mobile devices such as laptops or tablets unless such devices are kept on its premises at all times;

1.11 take reasonable steps to ensure the reliability of personnel who have access to the Personal Data;

1.12 have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Personal Data) including, but not limited to:

12.a.1 the ability to identify which individuals have worked with specific Personal Data;

12.a.2 having a proper procedure in place for investigating and remedying personal data breaches and breaches of the Data Protection Legislation; and

12.a.3 notifying the Data Controller as soon as any such breach occurs.

1.13 have a secure procedure for backing up all Personal Data, whether stored electronically or otherwise, enabling Personal Data to be restored in a timely fashion, and storing back-ups separately from originals;

1.14 have a secure method of disposal of unwanted Personal Data including for back-ups, disks, print-outs, and redundant equipment; and

1.15 adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001:2013, as appropriate to the Services provided to the Data Controller.

SCHEDULE 4

Legal Basis for Processing Personal Data Outside the EEA

The Data Sub Processor's legal basis for processing the Personal Data outside of the EEA in order to comply with cross-border transfer restrictions is as follows:

> Standard Contractual Clauses between the Data Controller as the "data exporter" and the Data Sub Processor as the "data importer".