

Data Processing Agreement

1. Agreement

- 1.1. **Application:** This Data Processing Agreement applies to the extent that Personal Data which is subject to EU Data Protection Law is Processed in the course of the performance of the Services. The Parties acknowledge and agree that with regard to such Processing of Personal Data, the customer is the Data Controller and Optimal is a Data Processor.
- 1.2. **Effective date:** This Data Processing Agreement is effective from the date it is signed by both Parties.
- 1.3. **Authority:** If the customer is using the Services on behalf of a business, the customer represents to Optimal that it has authority to bind that business or entity to this Data Processing Agreement and that the business accepts this Data Processing Agreement.
- 1.4. **Personal Data:** An overview of the categories of Personal Data, the types of Data Subjects, and purposes for which the Personal Data are being processed is provided in Annex 1.

2. Data Processing

- 2.1. **Data Controller's authority:** The Data Controller will, in determining the Services purchased and the Personal Data used in relation to those Services, determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor.
- 2.2. **Restrictions on processing:** The Data Processor will only process the Personal Data:
 - 2.2.1. on documented instructions of the Data Controller. This Data Processing Agreement constitutes the initial instructions and each use of the Services then constitutes further instructions. The Data Processor will use reasonable efforts to follow any later Data Controller instructions, as long as they are required by Data Protection Law, technically feasible and do not require changes to the Services. If the Data Processor otherwise cannot comply with an instruction or is of the opinion that an instruction infringes the GDPR or Applicable Data Protection Law, the Data Processor will immediately notify the Data Controller; or
 - 2.2.2. to comply with a legal obligation to which the Data Processor is subject. In such a case, the Data Processor shall inform the Data Controller of that legal obligation before processing, unless that law explicitly prohibits the furnishing of such information to the Data Controller.
- 2.3. **Customer Agreement and discretion:** The Parties have entered into a Customer Agreement in order to benefit from the expertise of the Data Processor in securing and processing the Personal Data for the purposes of the supply of the Services. The Data Processor may exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this Data Processing Agreement.
- 2.4. **Data Controller warranty:** The Data Controller warrants that it has all necessary rights to provide the Personal Data to the Data Processor for the Processing to be performed

in relation to the Services. To the extent required by the Applicable Data Protection Law, the Data Controller is responsible for ensuring that any necessary data subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. If such consent is revoked by the data subject, the Data Controller is responsible for removing the relevant Personal Data from the Services.

3. Confidentiality

3.1. Personal Data confidential: The Data Processor shall:

- 3.1.1. treat all Personal Data as strictly confidential;
- 3.1.2. inform all its employees, agents and/or Sub-processors engaged in processing the Personal Data of the confidential nature of the Personal Data; and
- 3.1.3. ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

4. Security

4.1. **Technical and organisational measures:** The Data Processor shall implement and maintain the Technical and Organisational Measures. The Data Controller agrees that it has reviewed the Technical and Organisational Measures. Each party acknowledges that it considers the Technical and Organisational Measures to be appropriate, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, taking account all the risks that are presented by processing, in particular from a Personal Data Breach.

4.2. **Types of Personal Data:** The Data Controller acknowledges that the Data Processor does not review the types of Personal Data collected in relation to the Services. If the Data Controller submits Personal Data to the Services that is not specified in Annex 1, the Data Controller agrees that it is responsible if the Technical and Organisational Measures do not meet the GDPR standard of appropriateness.

4.3. **Changes to measures:** The Data Processor may change the Technical and Organisational Measures at any time without notice so long as it maintains a comparable or better level of security. The Parties will negotiate in good faith the cost, if any, to implement changes required by specific updated security requirements in Applicable Data Protection Law or by data protection authorities of competent jurisdiction.

4.4. **Login details:** The Data Controller shall keep its login details confidential and secure and will not share them with others. If the Data Controller knows or suspects that its login information has or is likely to become used in an unauthorized way it shall immediately change its password or notify the Data Processor if it cannot change its password.

4.5. **Directions:** The Data Controller shall promptly comply with all reasonable directions issued by the Data Processor in relation to security or the Services.

5. Demonstration and audit

- 5.1. **Demonstration:** At the request of the Data Controller, the Data Processor shall make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR.
- 5.2. **Audit:** The Data Controller shall be entitled on giving at least 14 days' notice to the Data Processor to carry out, or have carried out by a third party who has entered into a confidentiality agreement with the Data Processor, audits of the Data Processor's premises and operations as these relate to the Personal Data. The Data Processor shall cooperate with such audits carried out by or on behalf of the Data Controller and shall grant the Data Controller's auditors reasonable access to any premises and devices involved with the Processing of the Personal Data. The Data Processor shall provide the Data Controller and/or the Data Controller's auditors with access to any information relating to the Processing of the Personal Data as may be reasonably required by the Data Controller to ascertain the Data Processor's compliance with this Data Processing Agreement.

6. Personal Data Breach

- 6.1. **Notifications:** The Data Processor shall notify the Data Controller without undue delay upon becoming aware of a Personal Data Breach affecting Personal Data, providing Data Controller with sufficient information to allow the Data Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Applicable Data Protection Laws. Such shall contain:
 - 6.1.1. a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
 - 6.1.2. the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;
 - 6.1.3. a description of the likely consequences of the incident; and
 - 6.1.4. a description of the measures taken or proposed to be taken by the Data Processor to address the incident including, where appropriate, measures to mitigate its possible adverse effects.
- 6.2. **Co-operation:** The Data Processor shall co-operate with the Data Controller and take such reasonable commercial steps as are directed by Data Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7. Contracting with Sub-Processors

- 7.1. **Authorisation:** The Data Processor lists the Sub-processors on its Website, including the name, address and role of each Sub-processor. The Data Controller authorises the engagement of such Sub-processors.
- 7.2. **Changes:** Where the Data Processor removes, adds or replaces a Sub-processor, it will update the list on the Website, thereby giving the Data Controller the opportunity to object to such changes. If the Data Controller objects to such changes to the sub-processors, its sole remedy is to cancel or terminate its account or the Services.
- 7.3. **Liability:** Notwithstanding authorisation by the Data Controller in accordance with this clause 7, the Data Processor shall remain fully liable vis-à-vis the Data Controller for

the performance of any such subprocessor that fails to fulfil its data protection obligations.

- 7.4. **Sub-processor obligations:** The Data Processor shall ensure that where it engages a Sub-processor for carrying out specific processing activities on behalf of the Data Controller, it will impose the data protection obligations as set out in this Data Protection Agreement as referred to in paragraph 3 of Article 28 of the GDPR on that Sub-processor, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR.
- 7.5. **Transfer:** The Data Processor may transfer information to multiple countries as part of providing Services. If information originates from the European Economic Area (“EEA”) the Data Processor will not transfer the information outside of the EEA unless it has taken such measures as are necessary to ensure the transfer is compliance with the EU Data Protection Law.
- 7.6. **Requests from data subjects:** The Data Processor shall promptly notify Data Controller if any Sub-processor receives a request from a Data Subject under any Data Protection Law in respect of Personal Data and ensure that the Sub-processor does not respond to that request except on the documented instructions of Data Controller or as required by Applicable Data Protection Laws to which the Sub-processor is subject, in which case Data Processor shall to the extent permitted by Applicable Laws inform Data Controller of that legal requirement before the Sub-processor responds to the request.

8. Data Transfers

- 8.1. **Transfers:** The Data Processor shall be entitled to process Personal Data, including by using Subprocessors, outside the country in which the Data Controller is located as permitted under Data Protection Law. Where the Data Processor transfers Personal Data to a country outside of the European Economic Area without an adequate level of protection, it lists such transfers on its Website. The Data Controller authorises such transfers. If the Data Controller objects to such transfers, its sole remedy is to cancel or terminate its account or the Services.
- 8.2. **Statutory mechanism:** To the extent that the Data Controller or the Data Processor are relying on a specific statutory mechanism to normalize international data transfers that are subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, the Data Controller and the Data Processor agree to cooperate in good faith to promptly terminate the transfer or to pursue a suitable alternate mechanism that can lawfully support the transfer.

9. Returning or Destruction of Personal Data

- 9.1. **Deletion or destruction:** The Data Processor shall at the choice of the Data Controller, delete or return all the Personal Data to the Data Controller after the end of the provision of the Services, and delete existing copies subject to clause 9.3.
- 9.2. **Return:** The Data Controller agrees that return of Personal Data shall be undertaken by the Data Controller exporting the applicable Personal Data from the Services prior to any termination of the Services.

- 9.3. **Retained data:** The Data Processor may retain Personal Data to the extent and for such period as required by applicable laws (for example, applicable New Zealand tax laws). The Data Processor shall ensure the confidentiality of all such retained Personal Data.
- 9.4. **Notification of third parties:** The Data Processor shall notify all third parties supporting its own processing of the Personal Data of the termination of the Data Processing Agreement and shall ensure that all such third parties shall either destroy the Personal Data or return the Personal Data to the Data Controller, at the discretion of the Data Controller.

10. Assistance to Data Controller

- 10.1. **Technical and organisational measures:** The Data Processor shall assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the data subject's rights under EU Data Protection Law.
- 10.2. **Assistance:** The Data Processor shall assist the Data Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR taking into account the nature of processing and the information available to the Data Processor.
- 10.3. **Impact assessments:** The Data Processor shall provide reasonable assistance to the Data Controller for any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Data Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other data protection law, in each case solely in relation to Processing of Personal Data by the Data Processor, and taking into account the nature of the Processing and information available to the Data Processor. The Data Processor may charge for such assistance at its standard rates.

11. Records

- 11.1. Each party is responsible for its compliance with its documentation requirements in particular maintaining records of processing where required under Applicable Data Protection Law. Each party shall reasonably assist the other party in its documentation requirements, including providing the information that the other party reasonably requests (such as through use of the Services), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

12. Liability

- 12.1. **Data subjects:** The Parties agree that any Data Subject who has suffered damage as a result of any breach of this DPA may be entitled to seek compensation either from the Data Controller or the Data Processor. If the one Party has paid damages that are partly or fully attributable to the other Party, the former is entitled to claim back the relevant part of the damages from the latter.

13. Duration and Termination

- 13.1. **Confidentiality:** Termination or expiration of this Data Processing Agreement shall not discharge the Data Processor from its confidentiality obligations pursuant to clause 3.

13.2. **Effective date:** The Data Processor shall process Personal Data until the earlier of:

13.2.1. the date of termination of the Customer Agreement;

13.2.2. any date that the Data Controller instructs that Processing cease; or

13.2.3. the return or destruction of all Personal Data in accordance with clause 9.

14. Variations

14.1. **Changes due to Applicable Data Protection Law:** Either Party may propose variations to this Data Processing Agreement if it reasonably considers it to be necessary to address the requirements of any Applicable Data Protection Law. If either Party gives such notice, the Parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the identified requirements as soon as is reasonably practicable.

14.2. **Changes due to Controller instruction:** Where an amendment to the Customer Agreement or this Data Protection Agreement is necessary in order to execute a Data Controller instruction to the Data Processor including to improve security measures:

14.2.1. the Parties shall promptly discuss the proposed instruction and negotiate in good faith as soon as is reasonably practicable with a view to agreeing and implementing instruction; and

14.2.2. if the Parties are not able to reach agreement, the Data Controller's sole remedy is to cancel or terminate its account or the Services.

15. Notices

15.1. **Contract details:** Each Party will deliver all notices under this Data Processing Agreement to addresses specified in Annex 2.

16. Miscellaneous

16.1. **Conflict in terms:** In the event of any conflict between this Data Processing Agreement and the Customer Agreement, this Data Processing Agreement will take precedence.

16.2. **Governing law:** This Data Processing Agreement is governed by the laws of New Zealand, and each party irrevocably submits to the non-exclusive jurisdiction of the New Zealand courts.

17. Interpretation and definitions

17.1. **Interpretation:** In these Terms, unless the context otherwise requires:

17.1.1. the singular includes the plural and vice versa;

17.1.2. a reference to materials means a reference to materials of any kind whether in the form of documentation, software or otherwise;

17.1.3. a reference to either party includes reference to its respective successors in title and permitted assigns (and where the context so permits) its personnel and representatives;

- 17.1.4. any agreement not to do a thing also constitutes an agreement not to suffer or permit or cause that thing to be done;
- 17.1.5. the words “includes” and “including” are to be read as being followed by the words “without limitation”; and
- 17.1.6. a reference to any documentation and the Website includes as varied or substituted.

17.2. Defined terms:

17.2.1. Terms such as **Processing** and **Personal Data Breach** have the meaning ascribed to them in the GDPR.

17.2.2. In addition:

Applicable Data Protection Law means all applicable data protection and privacy laws including, where applicable, EU data protection law or New Zealand privacy law.

Customer Agreement means the Terms of Service or, if the Parties have entered into a separate written agreement for the supply and use of the Services and the Website, that written agreement, each of which addresses the supply of Services to the customer.

Data Controller has the meaning given to “Controller” in the GDPR.

Data Processor has the meaning given to “Processor” in the GDPR.

EU Data Protection Law means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

GDPR means Directive 95/46/EC (General Data Protection Regulation) of EU Data Protection Law.

Optimal means Optimal Workshop Limited (New Zealand Registered Company number 1973791) and includes its successors and assigns, related companies, officers, directors, employees and agents.

Parties means the customer and Optimal.

Personal Data means such personal data (as that term is defined in the GDPR) as is provided by the Data Controller to the Data Processor for the purposes of the Data Processor providing the Services.

Services means the user research services supplied by Optimal under a Customer Agreement.

Sub-processor means a processor engaged by Optimal for carrying out specific processing activities on the customer’s behalf.

Technical and Organisational Measures means the technical and organisational measures outlined on the Website.

Website means the Optimal Workshop website at optimalworkshop.com.

Execution

Executed as an agreement:

[Customer]

Signature _____

Name _____

Title _____

Date Signed _____

Optimal Workshop Limited

Signature S. Janaki_____

Name Janaki Sabapathipillai_____

Title Project Manager, Security and Legal _____

Date Signed 09/07/18_____

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Personal Data

The subject matter and duration of the Processing of the Personal Data are set out in the principal part of this Data Processing Agreement.

Categories of Data Subject to whom the Personal Data relates

Data Controller may submit Personal Data to the Optimal Workshop tools, the extent of which is determined and controlled by the Data Controller in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Survey participants
- Data Controller's Users as authorised by Data Controller to use the Services

Categories of data

Data Controller may submit Personal Data to the Optimal Workshop tools, the extent of which is determined and controlled by the Data Controller in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Anonymised demographic data (no respondent identifiable) and ranking submissions
- Email address of authorized users

Special categories of data/data regarding minors or criminal history (if appropriate)

Data Controller may submit special categories of data or data regarding minors or criminal history to the Services, the extent of which is determined and controlled by the Data Controller in its sole discretion. Such data includes, for the sake of clarity, Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Processing operations

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Customer Agreement.

ANNEX 2: CONTACT DETAILS

Contact information of the [data protection officer/compliance officer] of the Data Controller:

Jlarevisionknee@gmail.com

data-protection@bristol.ac.uk

Contact information of the Data Protection Officer of the Data Processor:

privacy@optimalworkshop.com

Contact information for support requests: support@optimalworkshop.com