DATA PROCESSING AGREEMENT

This Data Processing Agreement (**Agreement**) forms part of the Services Agreement (**Services Agreement**) entered into by you (**Controller**) and PPC Protect Limited (company number 10359736), with its registered office at 3rd Floor, 1 Ashley Road, Altrincham, Cheshire, WA14 2DT, United Kingdom (**Processor**).

BACKGROUND

(A) The Services Agreement requires the Processor to process Personal Data on behalf of the Controller.

(B) This Agreement sets out the additional terms, requirements and conditions on which the Processor will process Personal Data when providing services under the Services Agreement. This Agreement contains the mandatory clauses required by Article 28(3) of the retained EU law version of the General Data Protection Regulation (*(EU) 2016/679*) for contracts between controllers and processors and the General Data Protection Regulation (*(EU) 2016/679)*.

AGREED TERMS

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Business Purposes: the services to be provided by the Processor to the Controller as described in the Services Agreement and any other purpose specifically identified in Annex A.

Commissioner: the Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018).

Controller means an entity that determines the purpose and means of Processing of the Personal Data.

Data Protection Legislation: means all applicable laws, regulations and regulatory requirements relating to the use, protection and privacy of Personal Data including, without limitation:

a) United Kingdom: the UK General Data Protection Regulation, the Data Protection Act 2018 and the Privacy And Electronic Communications Regulations 2003, in each case as amended or replaced from time to time

b) European Union: the EU General Data Protection Regulation, the EU e-Privacy Directive and all applicable national laws implementing or supplementing the same

c) United States: the California Consumer Privacy Act of 018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA), the Virginia Consumer Data Protection act (VCDPA), the Connecticut Data Privacy Act (CTDPA), the Colorado Privacy Act (CPA), the Utah Consumer Privacy Act (UCPA) and any other similar state-level privacy laws in force or enacted during the term of this Agreement

Data Subject: the identified or identifiable living individual to whom the Personal Data relates.

EU GDPR: the General Data Protection Regulation ((EU) 2016/679).

EU Standard Contractual Clauses (EU SCCs): the standard contractual clauses for the transfer of Personal Data to third countries adopted by the European Commission under Article 46 of the EU GDPR, as may be amended or replaced from time to time.

EEA: the European Economic Area.

International Data Transfer Agreement (IDTA): The standard form of Agreement issued by the UK Information Commissioner's Office for restricted transfers of Personal Data from the UK, or as amended or replaced from time to time.

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Processor on behalf of the Controller as a result of, or in connection with, the provision of the services under the Services Agreement; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Processing, processes, processed, process: any activity that involves the use of the Personal Data. It includes, but is not limited to, any operation or set of operations which is performed on the Personal Data or on sets of the Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring the Personal Data to third-parties.

Personal Data Breach: a breach of security leading to the accidental, unauthorised or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data.

Processor: a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.

Records: has the meaning given in Clause 13.

Sub-Processor: means any third party appointed by or on behalf of the Processor to process Personal Data on behalf of the Controller in connection with the Processor's provision of services under this Agreement. This includes any subcontractor or service provider engaged to carry out specific processing activities, excluding employees or direct contractors of the Processor.

Term: this Agreement's term as defined in Clause 11.

UK Addendum: The addendum issued by the UK Information Commissioner's Office to the EU SCCs, or any replacement or successor document, for transfers of Personal Data from the UK to third countries.

UK GDPR: has the meaning given in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

1.2 This Agreement is subject to the terms of the Services Agreement and is incorporated into the Services Agreement. Interpretations and defined terms set forth in the Services Agreement apply to the interpretation of this Agreement.

1.3 The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.

1.4 Changes to this Agreement must be agreed in writing in an amendment Agreement signed by both parties. A reference to writing or written includes e-mail.

1.5 In the case of conflict or ambiguity between:

a) any provision contained in the body of this Agreement and any provision contained in the Annexes, the provision in the body of this Agreement will prevail;

b) the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail; and

c) any of the provisions of this Agreement and the provisions of the Services Agreement, the provisions of this Agreement will prevail.

2. Personal Data types and processing purposes

2.1 The Controller and the Processor agree and acknowledge that for the purpose of the Data Protection Legislation:

a) the Controller is the Controller, and the Processor is the Processor;

b) the Controller retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Processor; and

c) Annex A describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Processor may process the Personal Data to fulfil the Business Purposes.

3. Controller’s Obligations

3.1 The Controller shall ensure that it has all necessary lawful bases (e.g. consent, legitimate interest) for the collection and processing of Personal Data.

3.2 The Controller shall provide the Processor with clear, lawful and documented processing instructions.

3.3 The Controller shall ensure that the Personal Data is accurate, complete and up to date.

3.4 The Controller shall comply with all applicable Data Protection Legislation in respect of its processing of personal data and its instructions to the Processor.

3.5 The Controller shall notify the Processor without undue delay of any errors or inaccuracies in the Personal Data.

3.6 The Controller shall inform Data Subjects, where required, about the sharing of their Personal Data with the Processor and ensure transparency obligations are met.

3.7 The Controller shall not instruct the Processor to perform any processing that would breach applicable Data Protection Legislation.

3.8 Where the Controller is subject to US state privacy laws (including but not limited to the California Consumer Privacy Act of 018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA), the Virginia

Consumer Data Protection act (VCDPA), the Connecticut Data Privacy Act (CTDPA), the Colorado Privacy Act (CPA), the Utah Consumer Privacy Act (UCPA)) and other similar legislation, the Controller shall:

a) inform the Processor of any specific obligations or restrictions arising under applicable state laws that may affect the processing of Personal Data;

b) ensure that its instructions to the Processor are compliant with all applicable US federal and state privacy laws; and

c) co-operate with the Processor to enable compliance with such laws, including providing necessary information or documentation.

3.9 The Processor shall process Personal Data in accordance with the Controller's lawful instructions and assist the Controller, where reasonably required, in meeting its obligations under applicable US privacy laws.

4. Processor's obligations

4.1 The Processor will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Controller's written instructions. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. The Processor will promptly notify the Controller if, in its opinion, the Controller's instructions do not comply with the Data Protection Legislation.

4.2 The Processor will comply promptly with any Controller written instructions requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

4.3 The Processor shall, at no additional cost to the Controller, assist the Controller in responding to Data Subject rights requests under applicable Data Protection Legislation, including access, rectification, erasure, restriction, portability, objection and rights related to automated decision-making. Such assistance shall be provided:

a. promptly upon written instructions from the Controller;

b. using appropriate technical and organisational measures; and

c. in a manner that enables the Controller to meet its obligations within the statutory timeframes.

The Processor shall not respond directly to any data subject request unless expressly authorised to do so by the Controller or required by law. If the Processor receives a request directly from the Data Subject, it shall promptly notify the Controller and forward the request without undue delay

4.4 The Processor will maintain the confidentiality of the Personal Data and will not disclose the Personal Data to third parties unless the Controller or this Agreement specifically authorises the disclosure, or as required by law, court or regulator (including the Commissioner). If a law, court or regulator (including the Commissioner) requires the Processor to process or disclose the Personal Data to a third party, the Processor will first inform the Controller of such legal or regulatory requirement and give the Controller an opportunity to object or challenge the requirement, unless the law prohibits the giving of such notice.

4.5 The Processor will reasonably assist the Controller, at no additional cost to the Controller, with meeting the Controller's compliance obligations under the Data Protection Legislation, taking into account the nature of the Processor's processing and the information available to the Processor, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with the Commissioner or other relevant regulator under the Data Protection Legislation.

5. Processor's employees

5.1 The Processor will ensure that its employees:

a) are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data; and

b) undertake security awareness training on a regular basis.

6. Security

6.1 The Processor will, at all times, implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Annex B**Error! Bookmark not defined.**. The Processor will periodically review its security measures, at least annually to ensure they remain current and complete.

6.2 The Processor will implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

a) the pseudonymisation and encryption of Personal Data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

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

d) a process for regularly testing, assessing and evaluating the effectiveness of the security measures.

7. Personal Data breach

7.1 The Processor will immediately inform the Controller in writing if it becomes aware of:

a) the loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data; the Processor will restore such Personal Data at its own expense as soon as possible;

b) any accidental, unauthorised or unlawful processing of the Personal Data; or

c) any Personal Data Breach.

7.2 Where the Processor becomes aware of (a), (b) and/or (c) above, it will, as soon as reasonably possible, also provide the Controller with the following written information:

a) description of the nature of (a), (b) and/or (c), including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

b) the likely consequences; and

c) a description of the measures taken or proposed to be taken to address (a), (b) and/or (c), including measures to mitigate its possible adverse effects.

7.3 Immediately following any accidental, unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. Further, the Processor will reasonably co-operate with the Controller at no additional cost to the Controller, in the Controller's handling of the matter, including but not limited to:

a) assisting with any investigation;

b) providing the Controller with physical access to any facilities and operations affected;

c) facilitating interviews with the Processor's employees, former employees and others involved in the matter including, but not limited to, its officers and directors;

c) making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Controller; and

d) taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or accidental, unauthorised or unlawful Personal Data processing.

7.4 The Processor will not inform any third party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Controller's written consent, except when required to do so by law. Where disclosure is required by law, the Processor shall (to the extent legally permitted) notify the Controller in advance of such disclosure, provide the Controller with a copy of the proposed communication, and limit the information disclosed strictly to what is legally required. In all cases, the Processor shall not reference the Controller or identify it as the Controller without the Controller’s prior written approval.

7.5 The Processor agrees that the Controller has the sole right to determine:

a) whether to provide notice of the accidental, unauthorised or unlawful processing and/or the Personal Data Breach to any Data Subjects, the Commissioner, other in-scope regulators, law enforcement agencies or others, as required by law or regulation or in the Controller's discretion, including the contents and delivery method of the notice; and

b) whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.

7.6 The Processor will cover all reasonable expenses associated with the performance of the obligations under Clause 7.1 to Clause 7.3 unless the matter arose from the Controller's specific written instructions, negligence, wilful default or breach of this Agreement, in which case the Controller will cover all reasonable expenses.

7.7 The Processor will also reimburse the Controller for actual reasonable expenses that the Controller incurs when responding to an incident of accidental, unauthorised or unlawful processing and/or a Personal Data Breach to the extent that the Processor caused such, including all costs of notice and any remedy as set out in Clause 7.5.

8. Transfers of Personal Data

8.1 The Processor shall not transfer Personal Data (nor permit its Sub-Processors to transfer Personal Data) outside the United Kingdom, the European Economic Area, or any country recognised as providing an adequate level of protection under Data Protection Legislation, except where:

a) the transfer is made on the documented instructions of the Controller; or

b) the transfer is required for the performance of the Services and is subject to an appropriate safeguard or transfer mechanism under Data Protection Legislation (including, as applicable, adequacy decisions, the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or the EU Standard Contractual Clauses); or

c) an exemption (derogation) under Article 49 UK GDPR / EU GDPR applies, provided that such reliance is exceptional and limited to the extent permitted by law.

8.2 In all cases, the Processor shall ensure that any such transfer (including by a Sub-Processor) is compliant with Data Protection Legislation and shall provide the Controller with reasonable information on request regarding such transfers.

8.3 Where SCCs (and the UK Addendum, where applicable) are required for restricted transfers, the Processor will ensure that such safeguards are in place and comply with the form and requirements prescribed under applicable Data Protection Legislation.

8.4 The Processor will provide the Controller with copies of the relevant transfer mechanism documentation upon request.

8.5. Where the processing involves the transfer of Personal Data to jurisdictions outside of the UK or EEA that do not benefit from an adequacy decision, the parties agree that the EU Standard Contractual Clauses (as adopted by the European Commission) and the UK Addendum (as issued by the UK ICO) filed at the *Lunio Trust Center* under 'Security and Other Documentation' shall apply and are incorporated by reference to this Agreement. By signing this Agreement, both parties confirm that they have read, understood and agreed to the terms of the EU SCCs and the UK Addendum, and shall comply with their respective obligations under those instruments.

9. Sub-Processors

9.1 In addition to the Sub-Processors set out in Annex A, the Processor is granted general authorisation to engage sub-processors for the performance of its obligations under this Agreement.

9.2 The Processor shall maintain an up-to-date list of Sub-Processors and shall notify the Controller in advance of any intended changes concerning the addition or replacement of Sub-Processors.

9.3 The Controller shall have the right to object to such changes on reasonable grounds related to data protection.

9.4 Where the Processor engages a Sub-Processor, it shall ensure that the Sub-Processor is bound by a written agreement that imposes the same data protection obligations as set out in this Agreement.

9.5 The Processor remains fully liable to the Controller for the performance of the Sub-Processor's obligations.

9.6 The parties agree that the Processor will be deemed to control legally any Personal Data controlled practically by, or in the possession of, its Sub-Processors.

10. Complaints, data subject requests and third party rights

10.1 The Processor will, at no additional cost to the Controller, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Controller as the Controller may reasonably require, to enable the Controller to comply with:

a) the rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase Personal Data, object to the processing and automated processing of Personal Data, and restrict the processing of Personal Data; and

b) information or assessment notices served on the Controller by the Commissioner or other relevant regulator under the Data Protection Legislation.

10.2 The Processor will notify the Controller immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

10.3 The Processor will notify the Controller as soon as possible but within 2 business days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

10.5 The Processor will give the Controller, at no additional cost to the Controller, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

10.6 The Processor will not disclose the Personal Data to any Data Subject or to a third party other than in accordance with the Controller's written instructions, or as required by law.

11. Term and termination

11.1 This Agreement will remain in full force and effect so long as the Services Agreement remains in effect (**Term**).

11.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Services Agreement in order to protect the Personal Data will remain in full force and effect.

11.3 A breach by either party of the terms of this Agreement shall constitute a breach of the Services Agreement.

12. Data return and destruction

12.1 At the Controller's request, the Processor will give the Controller, or a third party nominated in writing by the Controller, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Controller.

12.2 On termination of the Services Agreement for any reason or expiry of its term, the Processor shall retain any Personal Data in its possession or control that relates to this Agreement for a period of twelve (12) months unless otherwise instructed in writing by the Controller or as required by applicable law.

12.3 If any law, regulation, or government or regulatory body requires the Processor to retain any documents, materials or Personal Data that the Processor would otherwise be required to return or destroy, it will notify the Controller in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

12.4 The Processor will certify in writing to the Controller that it has deleted or destroyed the Personal Data within 5 business days after it completes the deletion or destruction.

13. Records

13.1 The Processor will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved Sub-Processors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures referred to in Clause 0 (the "**Records**").

13.2 The Processor will ensure that the Records are sufficient to enable the Controller to verify the Processor's compliance with its obligations under this Agreement and the Data Protection Legislation and the Processor will provide the Controller with copies of the Records upon request.

14. Audit

14.1 The Processor will permit the Controller and its third party representatives to audit the Processor's compliance with its obligations under this Agreement, on at least 30 days' notice, during the Term. The Processor will give the Controller and its third party representatives all reasonable assistance to conduct such audits at no additional cost to the Controller.

14.2 The notice requirements in Clause 14.1 will not apply if the Controller reasonably believes that a Personal Data Breach has occurred or is occurring, or the Processor is in material breach of any of its obligations under this Agreement or any of the Data Protection Legislation.

14.3 If a Personal Data Breach occurs or is occurring, or the Processor becomes aware of a breach of any of its obligations under this Agreement or any of the Data Protection Legislation, the Processor will:

a) immediately conduct its own audit to determine the cause;

b) produce a written report that includes detailed plans to remedy any deficiencies identified by the audit;

c) provide the Controller with a copy of the written audit report; and

d) remedy any deficiencies identified by the audit as soon as possible but no later than 7 days (unless otherwise agreed by the Controller).

15. Warranties

15.1 The Processor warrants and represents that:

a) it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

b) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to:

(i) the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage;

(ii) the nature of the Personal Data protected; and

(iii) comply with all applicable Data Protection Legislation and its information and security policies, including the security measures required in Clause 6.1.

15.2 The Controller warrants and represents that the Processor's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Controller will comply with the Data Protection Legislation.

16. Liability and Indemnification

16.1 This Agreement is subject to the indemnification and limitation of liability provisions of the Services Agreement.

17. Governing Law and Jurisdiction

17.1 This Agreement shall be governed by the laws of England and Wales.

3.2 All disputes shall be subject to the exclusive jurisdiction of the courts of England and Wales.

Annex A - Personal Data processing purposes and details

Subject matter of processing:

Interactions with paid media and organic web traffic.

Duration of Processing:

For the duration of the Services Agreement.

Nature of Processing:

Data collection, analysis and storage.

Business Purposes:

Fraud detection and prevention purposes.

Personal Data & Non-Personal Data Categories:

The Processor may process the following categories of data, as instructed by the Controller, for the purposes of fraud detection and prevention and the preservation of service integrity:

- Environment-related information (device type, operating system, locale setting)
- Browser features (plugins, history length, cookie enabled)
- Resources (timing metrics, response times)
- Math operations (duration calculation)
- Navigation (method, timing)
- Printing (visual rendering)
- Fingerprinting (audio, canvas, errors)
- WebGL (capability, hardware metadata, rendering context)
- Screen (dimensions, pixel depth, touch capabilities, orientation)
- CSS (user interface, layout and rendering, display characteristics)
- Battery (availability, charge level)
- Development (Runtime environment, storage media interface metadata)
- Bot mitigation (automated access signals, execution characteristics, browser anomalies)
- Older browser properties (legacy features, execution environment metadata)
- User interaction (mouse movement)

The categories listed above are provided for illustrative purposes only and do not represent an exhaustive list of the data processed under this Agreement.

For a complete and detailed list of data categories and processing activities, the Controller may access the Processor's secure Trust Centre at *Lunio Trust Center* . You may be asked to verify your identity using your business e-mail address.

Data Subject Types:

Prospective users or site visitors who interact with the Controller’s advertising and web assets.

Approved Sub-Processors:

Sub-Processor Name	Data Location
Amazon Web Services	United Kingdom
Slack	United States
Datadog	European Economic Area
Jiminny	United Kingdom
Salesloft	United States
Intercom	European Economic Area
Zoom	United States
Google Gmail	European Economic Area
Google Forms	European Economic Area
Google Meets	European Economic Area
Google Drive	European Economic Area

Annex B - Security Measures

The Processor shall implement and maintain appropriate technical and organisation measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the UK GDPR / EU GDPR. These measures are designed to protect personal data against unauthorised or unlawful processing, accidental loss, destruction or damage.

1. Access Control

- Role-based access restrictions to system data
- Authentication mechanisms including password policies and where applicable, multi-factor authentication
- Logging and monitoring of access to personal data

2. Data Transmission & Storage

- Encryption of personal data in transit using industry standard protocols (e.g. TLS)
- Secure storage environments with access restrictions and regular patching
- Segregation of environments to prevent unauthorised access

3. System & Network Security

- Firewalls, intrusion detection/prevention systems and endpoint protection
- Regular vulnerability assessments and penetration testing
- Network segmentation and secure configuration practices

4. Operational Security

- Change management and incident response procedures
- Regular backups and disaster recovery planning
- Monitoring and alerting for suspicious activity

5. Organisational Measures

- Staff training on data protection and information security
- Confidentiality Agreements and access policies for personnel
- Internal policies governing data handling, retention and disposal

6. Audit & Assurance

- Periodic internal reviews of security controls
- Support for audits or inspections by the Controller, subject to reasonable notice and scope

7. Data Minimisation

- Collection and processing limited to data necessary for the specified purpose