TAAP
means business for apps

Data Processor Agreement

Client: as stated in the Order

Reference: 20230612.DPA

Version: 6.0

Last Update: 12th June 2023

Table of Contents

1 DEFINITIONS 4
2 PROCESSING OBJECTIVES 7
3 CONTROLLER'S OBLIGATIONS 7
4 PROCESSOR'S OBLIGATIONS 9
5 ALLOCATION OF RESPONSIBILITY 11
6 DUTY TO REPORT 11
7 SECURITY 11
8 AUDIT 12
9 DURATION AND TERMINATION 12
10 LIABILITY 12
11 MISCELLANEOUS 13
12 AGREEMENT SIGNATURE 14

BETWEEN

(1) TAAP LIMITED a company registered in England and Wales under company number 04962797 whose registered office is Kinetic Centre, Theobald Street, Borehamwood, Herts, WD6 4PJ; *and*

(2) Client Name and Address as stated in the Order

THE AGREEMENT

Consists of the following instruments:

- Data Processor Agreement;
- Order

RECITALS

A. Hereinafter collectively referred to as 'Parties' and individually 'Party',

B. The Parties agree that this Data Processor Agreement ("DPA") sets forth their obligations with respect to the processing and security of the Controllers Data and Personal Data in connection with an Order

C. the Controller determines the purposes and means of the Processing of Personal Data (as defined within Article 4.7 of the GDPR);

D. the Controller instructs the Processor to execute certain types of Processing in accordance with this Agreement;

E. the Processor has undertaken to comply with this Agreement and to abide by the technical measures enforced by the Controller to protect natural persons with regard to the Processing of Personal Data and on the free movement of such Data;

F. This Agreement is supplemental to any other separate agreement entered hereto between the Parties and introduces further contractual provisions to ensure the protection and security of data passed from the Controller to the Processor for Processing;

G. It is intended that the Processor will, in relation to the works to be performed as specified in an Order, complete a Data Mapping & Processing Activity Assessment Audit and/or DPIA and/or Privacy Notice where applicable;

H. The Data Mapping & Processing Activity Assessment Audit and/or Processors DPIA and/or Privacy Notice will contribute towards the Controller's DPIA and must be read in conjunction with this Agreement.

1 DEFINITIONS

Item	Meaning
Agreement	Documents that relate to the processing of personal data that may be defined within the Data Processor Agreement and Order
Compliance	The need to comply with legal requirements regarding data processes.
Consent	Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Controller (or Data Controller)	The organisation that in respect of this agreement determines the purposes for which and the manner in which any Data is, or is to be, processed.
Data	Any Information being collected or processed by the Data Processor on behalf of the Data Controller
Data Mapping & Processing Activity Assessment Audit	Custom document to identify personal data pertaining to a data subject and document the data lifecycle, including but not restricted to: why it's processed, when it's collected, where it's stored, who it's shared with and how it's protected. This is to assist with development of a DPIA by the Controller.
Data Protection Officer (DPO)	Is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data Protection Officer is responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with GDPR requirements.
Data Protection Regulation	The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the United Kingdom (UK)
Data Protection Regulator	Refer to Regulatory Authority. The UK Data Protection Regulator is the ICO
Data Security Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data
Data Subject	A data subject is any person whose personal data is being collected, held or processed.
DPIA	Stands for: Data Protection Impact Assessment.
Effective Date	Date the Order is entered into.
End User Client License / User License/ EULA Client	The user licences purchased by the End Clients which entitles Authorised Users to access and use the TAAP Software, Services and Documentation in accordance with Commercial Agreements.
GDPR	The UK General Data Protection Regulation (UK GDPR) is part of the data protection landscape that includes the Data Protection Act 2018 (the DPA 2018). The UK GDPR sets out requirements for how organisations need to handle personal data.

ICO	The Information Commissioner's Office, UK Data Protection Regulator, referred to also as the Supervisory Authority.
Legal Basis	The data protection law provides six legal bases for processing: consent, performance of a contract, a legitimate interest, a vital interest, a legal requirement, and a public interest.
Order	Commercial transaction confirmed through either a purchase order being issued or payment of an invoice.
Personal Data	Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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 that natural person.
Processing	Any operation or set of operations which is/are performed upon personal data, (whether or not by automatic means) including collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Such processing may be wholly or partly by automatic means or processing otherwise than by automatic means of personal data which form part of a filing system or one intended to form part of a filing system. A filing system shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis.
Processor (or Data Processor)	The Processor is the organisation that is in respect of this agreement processing the Data on behalf of the Data Controller.
Privacy Notice	Defines who is the Controller and Processor and outlines the Data being Processed, how it is being Processed, legal basis for Processing and Data Subjects rights specific to an Order.
Regulatory Authority	Referred to also as the Data Protection Regulator or Supervisory Authority; A regulatory authority is an autonomous authority or agency established by a federal, state or provincial government.
Rights of Individuals	The GDPR provides the following rights for individuals: The right to be informed; The right of access; The right to rectification; The right to erasure; The right to restrict processing; The right to data portability; The right to object; Rights in relation to automated decision making and profiling.
Services	Services include: Consultancy Services in the form of Project Management, Account Management, Development, Testing and Support utilised in order to implement and support the Solution.
Software	the TAAP Software products and applications that Client has selected to licence and are made available by TAAP as part of the Services, for a fee, as set out in the relevant Order
Sub-Processor	A Processor might wish to sub-contract all or some of the processing to another Processor. For shorthand this is sometimes referred to as using a 'sub-processor', although this term is not taken from the GDPR itself.

Technical and Organisational Measures	Are the functions, processes, controls, systems, procedures and measures taken to protect and secure the personal information that an organisation processes.
Third Party(ies)	"third party" means a natural or legal person, public authority, agency, or body other than the data subject, Controller, Processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

2 PROCESSING OBJECTIVES

2.1 The Processor undertakes to process Personal Data on behalf of the Controller in accordance with the conditions laid down in this Agreement and outlined by the Controller as part of the Order. The Processing will be executed exclusively within the framework of this Agreement, and for all such intent and purposes, as may be agreed to subsequently.

2.2 The Processor shall refrain from making use of the Personal Data for any purpose other than as specified by the Controller. The Controller will inform the Processor of any such purposes which are not contemplated in this Agreement or as outlined by the Controller as part of the Order.

2.3 All Personal Data processed by the Processor on behalf of the Controller shall remain the property of the Controller and/or the relevant Data Subject(s).

3 CONTROLLER'S OBLIGATIONS

3.1 The Controller warrants to the Processor that it will comply at all times with the Data Protection Regulation in the United Kingdom, referred to as The Data Protection Act 2018 (DPA), the UK's implementation of the General Data Protection Regulation (GDPR) and, to the extent applicable, the data protection or privacy laws of any other country.

3.2 The Controller shall comply with its obligations under this Agreement.

3.3 Compliance with the data protection principles: as Controller you must comply with the data protection principles listed in Article 5 of the GDPR. The Controller hereby warrants, represents, and undertakes that the Personal Data shall comply with the DPA and the GDPR in all respects including, but not limited to, its collection, holding, and processing, and that the Controller has in place all necessary and appropriate consents and notices to enable the lawful transfer of the Personal Data to the Processor.

3.4 Individuals' rights: as Controller you must ensure that individuals can exercise their rights regarding their personal Data, including the rights of access, rectification, erasure, restriction, Data portability, objection and those related to automated decision-making.

3.5 Security: as Controller you must implement appropriate technical and organisational security measures to ensure the security of personal Data.

3.6 Choosing an appropriate Processor: as Controller you can only use a Processor that provides sufficient guarantees that they will implement appropriate Technical and Organisational Measures to ensure their Processing meets GDPR requirements. This means you are responsible for assessing that your Processor is competent to process the Personal Data in line with the GDPR's requirements. This assessment should take into account the nature of the Processing and the risks to the Data Subjects.

3.7 Processor contracts: as Controller you must enter into a binding contract or other legal act with your Processors, which must contain a number of compulsory provisions as specified in Article 28(3) of the GDPR.

3.8 Notification of personal Data breaches: as Controller you are responsible for notifying personal Data breaches immediately to the ICO, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. You are also responsible for notifying affected individuals (if the breach is likely to result in a high risk to their rights and freedoms).

3.9 Accountability obligations: as Controller you must comply with the GDPR accountability obligations, such as maintaining records, carrying out data protection impact assessments and appointing a Data Protection Officer.

3.10 International transfers: as Controller you must comply with the GDPR's restrictions on transfers of personal Data outside the UK.

3.11 Co-operation with supervisory authorities: as Controller you must cooperate with supervisory authorities (such as but not limited to the ICO) and help them perform their duties.

3.12 Data protection fee: as Controller you must pay the ICO a data protection fee unless you are exempt.

4 PROCESSOR'S OBLIGATIONS

4.1 The Processor warrants to the Controller that it shall at all times during this Agreement comply with the Data Protection Regulation in the United Kingdom, referred to as The Data Protection Act 2018, the UK's implementation of the General Data Protection Regulation (GDPR) and, to the extent applicable, the data protection or privacy laws of any other country.

4.2 The Processor shall comply with its obligations under this Agreement and agrees to comply with any reasonable measures required by the 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 GDPR) and any best practice guidance issued by the ICO.

4.3 The Processor is only to carry out services, and only to process the Personal Data received from the Controller strictly in accordance with the express written authorisation and instructions of the Controller (which may be specific instructions or instructions of a general nature or as otherwise notified by the Controller to the Processor). All instructions given by the Controller to the Processor shall at all times be in compliance with the DPA, the GDPR and other applicable laws. The Processor shall act only on such instructions from the Controller unless the Processor is required by law to do otherwise.

4.4 Sub-processors: the Processor must not engage another Processor (i.e. a Sub-Processor) without the Controller's prior specific or general written authorisation. If authorisation is given, the Processor must put in place a contract with the Sub-Processor with terms that offer an equivalent level of protection for the Personal Data as those in the contract between the Processor and the Controller.

4.5 Security: the Processor must implement appropriate Technical and Organisational Measures to ensure the security of Personal Data, including protecting against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.

4.6 Notification of Personal Data breaches: if the Processor becomes aware of a Personal Data breach, the Processor must notify the relevant Controller without undue delay. The Processor must also assist the Controller in complying with its obligations regarding Personal Data breaches.

4.7 Notification of potential data protection infringements: the Processor must notify the Controller immediately if any of their instructions would lead to a breach of the GDPR or local data protection laws.

4.8 Accountability obligations: the Processor must comply with certain GDPR accountability obligations, such as maintaining records and appointing a Data Protection Officer.

4.9 The Processor shall promptly comply with any request from the Controller requiring the Processor to amend, transfer, delete, or otherwise dispose of the Personal Data.

4.10 International transfers: When processing the Personal Data on behalf of the Controller, the Processor shall not process the Personal Data outside the United Kingdom without the prior written consent of the Controller and, where the Controller consents to such a transfer to a country that is outside of the EEA, to comply with the obligations of Processors under the provisions applicable to transfers of Personal Data to third countries set out in Chapter 5 of the GDPR by providing an adequate level of protection to any Personal Data that is transferred.

4.11 Co-operation: the Processor is obliged to cooperate with supervisory authorities (such as the ICO) to help them perform their duties. The Processor shall provide all reasonable assistance (at the Controller's cost) to the 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.

4.12 The Processor shall, at the written request of the Controller, delete (or otherwise dispose of) the Personal Data or return it to the Controller in the format(s) reasonably requested by the Controller within a reasonable time after the earlier of the following: (i) the end of the provision of the services under the Agreement; or (ii) the processing of that Personal Data by the Processor is no longer required for the performance of the Processor's obligations under the Agreement.

5 ALLOCATION OF RESPONSIBILITY

5.1 The Processor is explicitly not responsible for other Processing of Personal Data, including but not limited to Processing for purposes that are not reported by the Controller to the Processor, and Processing by Third Parties and / or for other purposes.

5.2 The Controller represents and warrants that the contents are not unlawful and do not infringe any Rights of Individuals. In this context, the Controller indemnifies the Processor of all claims and actions of Third Parties related to the Processing of Personal Data without express Consent and/or Legal Basis under this Data Processing Agreement.

6 DUTY TO REPORT

6.1 In the event of a Data Security Breach the Processor shall, to the best of its ability, notify the Controller thereof with undue delay and shall cooperate fully with the Controller and assist as required in relation to any subject access request, complaint, or other request..

6.2 The Processor will endeavour that the provided information is complete, correct and accurate, and will include:

a) the (suspected) cause of the Data Security Breach;

b) the (currently known and/or anticipated) consequences thereof;

c) the (proposed) solution;

d) the measures that have already been taken.

7 SECURITY

7.1 The Processor will endeavour to take adequate Technical and Organisational Measures against loss or any form of unlawful Processing (such as unauthorised disclosure, deterioration, alteration or disclosure of Personal Data) in connection with the performance of Processing Personal Data under this Agreement as agreed with the Controller.

7.2 The Processor does not guarantee that the security measures are effective under all circumstances. The Processor will endeavour to ensure that the security measures are of a reasonable level, having regard to the state of the art, the sensitivity of the Personal Data and the costs related to the security measures.

7.3 The Controller shall make the Personal Data available to the Processor if it is assured that the necessary security measures have been taken.

8 AUDIT

8.1 An audit may only be undertaken when there are specific grounds for suspecting the misuse of Personal Data and lack of adherence to this Agreement, and no earlier than two weeks after the Controller has provided written notice to the Processor.

8.2 Any such audit will follow the Processor's reasonable security requirements and will not interfere unreasonably with the Processor's business activities.

8.3 The findings in respect of the performed audit will be discussed and evaluated by the Controller and Processor and, where applicable, resolution steps implemented accordingly.

8.4 The costs of the audit will be borne by the Controller.

9 DURATION AND TERMINATION

9.1 This Data Processing Agreement is entered into for the duration set out in the relevant Order.

9.2 The Data Processing Agreement may not be terminated in the interim.

10 LIABILITY

10.1 The Processor's liability to the Controller for any loss or damage of whatsoever nature suffered or incurred by the Controller related to this Agreement shall to the extent permitted by law not exceed £1000.

10.2 The Processor's liability to the Controller for any liability of the Controller to any other person for any loss or damage of whatsoever nature suffered or incurred by that person related to this Agreement shall to the extent permitted by law not exceed £1000.

10.3 Nothing in this Agreement 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 GDPR. Furthermore, the Processor hereby acknowledges that it shall remain subject to the authority of the ICO and shall co-operate fully therewith, as required, and that failure to comply with its obligations as a data processor under the GDPR may render it subject to the fines, penalties, and compensation requirements set out in the GDPR.

11 MISCELLANEOUS

11.1 The Data Processing Agreement and the implementation thereof will be governed by the laws of England and Wales.

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

11.3 TAAP reserves the right to amend this Agreement from time to time to ensure compliance with latest Data Protection Regulation and Data Protection Regulator's guidance

12 AGREEMENT SIGNATURE

The Parties hereto have caused this Data Processor Agreement to be executed on receipt of an Order.

TAAP Limited (the Processor)

Signature	
Name (Printed)	STEPHEN HIGGON
Title	CEO
Date	12th June 2023