Data Processing Agreement

APPTWEAK S.A.

The Data Processing Agreement contains the following sections:

This Data Processing Agreement ("DPA") forms part of the Terms of Services ("**Agreement**") between: (i) AppTweak, the Service provider or Data Processor **(**hereinafter **the "Processor" or** "**Vendor**"**)** acting on its own behalf and as agent for each Vendor Affiliate; and (ii) you, the Client or Data Controller (hereinafter **the "Controller" or "Client**") acting on its own behalf and as agent for each Client Affiliate.

Hereinafter jointly referred to as "**Parties**"**,**

HEREBY AGREE AS FOLLOWS:

Article 1 – Introduction

The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below form an integral part of the Agreement..

Article 2 - Subject

In the framework of their contractual relationship, the Parties agree to respect the Data Protection Laws concerning the processing of personal data and, in particular, the GDPR and the Belgian legislation implementing the GDPR, in particular the law of 30 July 2018.

The present DPA (together with the annexes, which form an integral part thereof) - as required by article 28 of the GDPR - defines the terms and conditions under which the Processor agrees to perform processing activities of Cllient Personal Data described below on behalf of the Controller.

Article 3 - Description of the processing activities

The Processor is authorised to process on behalf of the Controller the Client Personal Data required for the provision of the Service(s) as described in this article. It sets out certain information regarding the Contracted Processors' Processing of the Client Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws).

a) The subject matter and duration of the Processing of the Client Personal Data are set out in the Agreement and this DPA ;
b) The nature of the processing activities is, at the request of the Controller, the extraction by the Processor from Apple App Store and Google Play Stores, the storage and displaying of the Client Personal Data on the Processor's Solution.
c) The Processor is authorised to process on behalf of the Controller the personal data required to integrate some information containing personal data on the Vendor's Platform (to use « review management » integration), which allows the Controller to see, analyse and reply to reviews posted by Apple and Google Users (the « **Purpose** »).
d) The types of personal data to be processed are the username and ID of the Apple or the Google user;
e) The categories of Data Subject to whom the Client Personal Data relates are Apple and Google Users;
f) The obligations and rights of Client Affiliates are set out in the Agreement and this DPA.

Article 4 - Duration

The DPA enters into force and is concluded for the entire period of the Agreement between the Parties, of which it forms an integral part.

Article 5 - Obligations of the Processor

The Processor agrees to:

a) processes the personal data only on documented instructions from the Controller, at the risk of being considered as a controller in the sense of article 28.10 GDPR, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
b) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons;
c) take all measures required pursuant to Article 32 GDPR (security of processing), and to implement appropriate technical and organizational measures required under

the applicable Data Protection Laws to protect the Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. The processor represent that such measures provide a level of security appropriate to the risk represented by the processing and the nature of the Personal Data;

d) taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
e) assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR (security of processing, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment and prior consultation) taking into account the nature of processing and the information available to the Processor;
f) make available, upon first request of the Controller, all information necessary to demonstrate compliance with the obligations laid down in this article and allow for and contribute to audits within the terms of article 7, including inspections, conducted by the Controller or another auditor mandated by the Controller;

Article 6 – Audits

In the event of an audit, the following principles will be respected:

a) the Controller will only request one (1) audit per year maximum, unless the Processor seriously fails to fulfil its obligations, in which case the Controller may request an additional audit ;
b) the Controller will inform the Processor by registered letter with acknowledgement of receipt at least 6 weeks before the date of the planned audit and will include a detailed plan of its request in this notification. In the event of an audit following a serious breach committed by the Processor, the Controller will inform the Processor with forty-eight (48) hours' written notice.
c) It is expressly agreed that the following will not be subject to the audit: any financial or personal data that does not concern the Controller, any information whose disclosure would be likely to affect the security of the Processor’s systems and/or data (in which case the Processor must give reasons for its refusal on legitimate grounds, e.g. confidentiality or security issues) or of the Processor’s other customers, and the source code of the Processor’s software or of any other tool used by the Processor;
d) all costs relating to the audit, including the Processor's internal costs, shall be borne exclusively by the Controller;
e) the duration of the audit shall not exceed three (3) working days. The Processor shall send an invoice to the Controller for all costs resulting from this audit, including the working days of his staff, it being specified that the rate for one working day will be invoiced at the man-day rate mentioned in the contract concluded, or, failing this, one thousand (€1,000.00) euros excluding tax;
f) the auditor may not make copies of documents, files, data or information, in whole or in part, nor may he take photographs, digitize or capture sound, video or computer recordings; nor may he request that all or part of these elements be supplied or sent to him;
g) the Processor may arrange for the display of sensitive documents in a black room;
h) any auditor who is a natural person may only be admitted to a site of the Processor or of one of its Sub-Processors after the Controller has declared his/her identity;
i) the Controller must ensure the integrity of the auditors appointed, whether they are employees of the Controller or of an external audit firm, and the Controller guarantees the Processor that the auditor will respect the confidentiality obligations mentioned in the contract concluded;

j) the audit shall take place during the normal business hours of the Processor's offices and shall be conducted in such a way as not to hinder the performance of the Processor's entrusted service or the production for other clients of the Processor, which shall in any case take precedence over the performance of the audit; the Processor may at any time interrupt the audit if the production requires that the resources and means occupied by the audit be mobilised for other purposes.

Article 7 - Sub-processing

The Processor, subject to the provisions of this Article, is allowed to use processor ("**Sub-Processor"**) of its choice for carrying out specific processing activities.

In such case, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Processors.

The Sub-Processor must respect the obligations of the DPA on behalf of and in accordance with the instructions from the Controller by way of a contract or other legal act under EU or Member State law.

The Processor must ensure that the Sub-Processor provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where the Sub-Processor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the Sub-Processor's obligations.

Article 8 - Right of information and Data subject rights

It is up to the Controller to provide the information to data subjects concerning the processing activities at the moment the data is being collected.

To the extent possible, the Processor must assist the Controller to fulfil its obligation to respond to requests from data subjects exercising their data subject rights: right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability, right to object and automated individual decision-making (including profiling).

If a data subject contacts the Processor to exercise any of their rights, the Processor must transfer such a request to the Controller by email as soon as possible upon receiving the request by email at email address indicated in the user account.

Article 9 - Notification of a personal data breach

The Processor shall notify the Controller of any personal data breach without undue delay after becoming aware of a personal data breach by the following means: email. Such notification must be accompanied by all useful documents in order to allow the Controller, if required, to notify without undue delay the competent supervisory authority and/or the data subjects.

The decision of whether or not to inform the Supervisory Authority and or data subjects of a personal data breach is taken solely by the Controller.

Article 10 - Data Protection Impact Assessment

The Processor agrees to provide assistance to the Controller in the course of the achievement of Data Protection Impact Assessments and in the course of a prior consultation of the Supervisory Authority. Furthermore, the Processor shall assist the Controller to respond to requests of the Supervisory Authority.

Article 11 - Expiry

Upon expiry of the services relating to the processing of personal data, at Controller's choice and request, the Processor undertakes to destroy all Client Personal Data he is processing as a Processor; to return all Client Personal Data to the Controller or to return the Client Personal Data to the Sub-Processor designated by the Controller solely on the instructions of the Controller.

The return of Client Personal Data must be accompanied by the destruction of all existing copies within the systems of the Processor, unless Personal Data is processed by the Vendor as a Data Controller or unless Union or Member State law requires storage of the personal data. Upon their destruction, Processor must provide adequate proof thereof to the Controller.

The Controller shall retain the ownership (including intellectual ownership in the broadest sense) of all Client Personal Data and Integration data made available to the Processor in the context of the performance of this DPA.

Article 12 - Data protection officer

The Processor communicates the name and contact details of its data protection officer (DPO) to the Controller, as it has appointed such a person in accordance with article 37 GDPR.

Contact information of the DPO:

KaizenLaw

dpo@apptweak.com

Article 13 - Record of processing activities

Processor shall keep a record of processing activities that he performs on behalf of the Controller and shall provide this register to the supervisory authority or Controller upon simple request.

Article 14 - Obligations of the Controller

The Controller agrees to:

a) provide the data required for the performance of the DPA described in Article 4 to the Processor;
b) document in writing each instruction regarding the processing of personal data by the Processor;
c) ensure, both at the commencement and during the processing, to respect its obligations resulting from the GDPR and the present DPA;
d) supervise the processing, including by performing audits and inspections at the Processor if it deems this to be useful;
e) ensure that the processing of personal data, assigned to the Processor, has a valid legal basis;
f) provide the Processor with all the information necessary to identify and evaluate risks to the rights and freedoms of natural persons.

Article 15 - Various

The DPA expresses the entire agreement between the Parties concerning its subject matter and supersedes all previous agreement between the Parties in this regard. The DPA cannot be altered, unless in the event of a written agreement between the Parties.

In the event any provision of the DPA would be considered illegal, invalid or non-applicable, in whole or in part, such provision shall not be considered to form a part of the DPA and shall not affect the legality, validity or applicability of the DPA.

In such a case or in the event of a lacking legal mention, the Parties agree to negotiate immediately in good faith in order to install a new provision having an equivalent economic effect to the non-applicable or lacking provision.

The DPA is subject to and interpreted according to the applicable law as stated in the Agreement. Any dispute relating to its validity, interpretation or performance shall be brought before the exclusive jurisdiction of the courts as stated in the Agreement, if it cannot be resolved amicably between the Parties.

Article 16 – Definitions

In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

17.1. "**Client Affiliate**" means a Data Controller « Affiliate » that directly or indirectly controls, is controlled by, or is under common control with the Data Controller. Control shall mean ownership of more than 50% of the voting rights or the power to direct the management or policies of an entity;

17.2. "**Client Group Member**" means the Data Controller or any Client Affiliate;

17.3. "**Client Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Data Controller or Client Group Member pursuant to or in connection with the Agreement;

17.4. "**Contracted Processor**" means a Vendor or a Subprocessor;

17.5. "**EEA**" means the European Economic Area;

17.6. "**EU Data Protection Laws**" means EU General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 applicable as from 25 May 2018 (**"GDPR"**) and laws implementing or supplementing the GDPR;

17.7. "**Standard Contractual Clauses**" means the contractual clauses set out and pre-approved by the European commission that can be used to ensure appropriate data protection safeguards when transferring personal data outside the European Union and the EEA ;

17.8. "**Subprocessor**" means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Client Group Member in connection with the Agreement; and

17.9. "**Vendor Affiliate**" means a Data Processor « Affiliate ».

The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.