APPENDIX 2: DATA PROCESSING ADDENDUM

The Data Processing Addendum contains the following sections:

This Data Protection Addendum ("**DPA**”), its own annexes here below (Annex 1: the technical and organizational measures (“TOM’s”) and annex 2: the list of sub-processors), and where applicable, the **Standard Contractual Clauses** form an integral part of the Terms of Services, or where applicable, the License & Master Services Agreement ("**Principal Agreement**") between: (i) AppTweak, the Service provider and Data Processor (hereinafter the “**Processor**” or "**Vendor**") acting on its own behalf and as agent for each Vendor Affiliate; and (ii) you, the Client and 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 Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the

Principal Agreement. Except as modified below, the terms of the Principal 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 shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

Article 2 – Definitions

In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:
2.1. "Client **Affiliate**" means a Client or Data Controller « Affiliate » as defined in Appendix 1 : Terms and Conditions of the License and Master Services Agreement;
2.2. "Client **Group Member**" means the Data Controller, Company or any Company Affiliate;
2.3. "Client **Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Client Group Member pursuant to or in connection with the Principal Agreement;
2.4. "**Contracted Processor**" means Vendor or a Subprocessor;
2.5. "**EEA**" means the European Economic Area;
2.6. "**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;
2.7. "**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 ;
2.8. "**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 Principal Agreement; and
2.9. "**Vendor Affiliate**" means a Data Processor « Affiliate » as defined in Appendix 1 : Terms and Conditions of the License and Master Services Agreement.
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.

Article 3 - 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 Addendum (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 Client Personal Data described below on behalf of the Controller.

Article 4 - 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 Principal Agreement and this Addendum ;
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 and Client Affiliates are set out in the Principal Agreement and this Addendum.

Article 5 - Duration

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

Article 6 - 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 7 – 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 8 - 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 Addendum 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 9 - 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 10 - 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 11 - 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 12 - 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 Addendum.

Article 13 - 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: dpo@Apptweak.com

Article 14 - 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 15 - Obligations of the Controller

The Controller agrees to:

a. provide the data required for the performance of the Addendum 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 Addendum;
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 16 - Various

The Addendum expresses the entire agreement between the Parties concerning its subject matter and supersedes all previous agreement between the Parties in this regard. The Addendum cannot be altered, unless in the event of a written agreement between the Parties.
In the event any provision of the Addendum 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 Addendum and shall not affect the legality, validity or applicability of the Addendum.
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 Addendum is subject to and interpreted according to the applicable law as stated in the Principal Agreement. Any dispute relating to its validity, interpretation or performance shall be brought before the exclusive jurisdiction of the courts as stated in the Principal Agreement, if it cannot be resolved amicably between the Parties.

Annex 1 – Technical and Organizational Measures ("TOM's")

Introduction

The security measures listed in point I above warrant a level of security appropriate to the risk of the intended processing activities. In order to determine the adequate security measures, the Parties shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

These security measures are intended in particular to prevent any unauthorised collection or processing of personal data.If, due to any progression in the state of the art, important modifications would be required to the technologies used to secure the personal data, the Processor shall inform the Controller.
The Controller and Processor agree to take all reasonable efforts in order to ensure that their systems and processing activities comply with the confidentiality, integrity, availability and constant resilience requirements, taking into account the state of the art and the cost of implementation.

AppTweak's ISO/IEC 27001 certification underscores its commitment to safeguarding information assets through a robust Information Security Management System (ISMS). This document outlines the Technical and Organizational Methods (TOMs) derived from AppTweak's adherence to ISO standards to ensure the confidentiality, integrity, and availability of data. The measures described herein align with industry best practices and applicable regulatory requirements.

1. Organizational Controls

1.1. Information Security Policies

- AppTweak maintains a set of security policies that are developed, approved, and regularly reviewed.
- Policies align with ISO/IEC 27001 standards and organizational objectives.
- These policies cover acceptable use, data protection, access control, incident management, and risk management.

1.2. Governance and Risk Management

- Regular risk assessments are conducted to identify, evaluate, and mitigate information security risks.
- Risk treatment plans are implemented, with continuous monitoring of identified risks.
- An internal organization chart defines clear roles and responsibilities related to security.

1.3. Roles and Responsibilities

- AppTweak has appointed a **Chief Information Security Officer (CISO)** responsible for overseeing compliance and security improvements.
- A **Data Protection Officer (DPO)** is designated to ensure GDPR compliance.
- Employees with access to personal data are bound by confidentiality agreements.

1.4. Supplier and Partner Management

- Third-party suppliers must comply with AppTweak's security requirements through contractual agreements.
- Regular audits and assessments of third-party security practices are performed.
- Multi-factor authentication (MFA) is enforced for access to critical systems where applicable.

1.5. Business Continuity and Incident Management

- AppTweak maintains and tests a **Business Continuity Plan (BCP)** to ensure resilience in case of disruptions.
- A **disaster recovery plan** is in place to restore operations in case of system failure.
- An **incident response plan** ensures security breaches are effectively addressed.

2. People Controls

2.1. Training and Awareness

- Security awareness training is conducted yearly for all employees.

- Training sessions emphasize phishing awareness, password security, and incident reporting.

2.2. Pre-Employment Screening

- Employee backgrounds are verified before onboarding.
- Employment contracts include security responsibilities and confidentiality clauses.

2.3. Disciplinary Measures

- Formal procedures exist to handle violations of security policies.
- Measures include verbal and written warnings, up to contract termination if necessary.

3. Physical Controls

3.1. Access to Secure Areas

- Physical access to AppTweak offices is restricted to authorized personnel only.
- Offices are secured with **electronic access control systems and visitor logs**.
- **Security cameras (CCTV)** are deployed for monitoring and access control.

3.2. Equipment Security

- Workstations and servers are **secured against theft, damage, or misuse**.
- Secure disposal of redundant equipment follows a **hardware disposal process**.
- All corporate devices are encrypted and require authentication for access.

3.3. Environmental Security

- Data is stored in compliant data center:
    - areas are **monitored for temperature and humidity control**.
    - fire suppression systems and uninterruptible power supplies (UPS) are deployed to protect critical equipment.
    - measures are in place to prevent physical threats such as **fire and flooding**.

4. Technological Controls

4.1. System and Software Security

- **Regular updates** are applied to operating systems, software, and security tools.
- Vulnerability management is performed to identify and mitigate security flaws.
- Configuration of new and existing systems follows security best practices.

4.2. Access Management

- Role-Based Access Control (**RBAC**) is enforced to **limit access to data on a need-to-know basis**.
- Every user has a **unique login identifier**, and authentication is required.
- **Multi-Factor Authentication (MFA)** is enforced for accessing secret information.

4.3. Cryptographic Measures

- **Encryption is applied to data at rest and in transit** using industry-standard algorithms.
- **Network and mobile devices are encrypted** to prevent unauthorized access.

4.4. Network Security

- **Wi-Fi networks are secured with WPA2 encryption**.
- Access to internal systems requires **VPN with authentication**.

4.5. Endpoint and System Security

- Automated security updates are enabled for operating systems and applications.
- Accounts of former employees are **systematically deactivated** as part of the offboarding process.

4.6. Monitoring and Logging

- Continuous **monitoring of network traffic and system activity** is in place.
- Logs are retained in a **secure and tamper-evident format** for forensic analysis.

5. Compliance and Continuous Improvement

5.1. Internal Audits

- Regular audits assess compliance with ISO/IEC 27001 and regulatory requirements.
- Audit findings are documented, and corrective actions are implemented.

5.2. Regulatory Compliance

- Compliance with **GDPR and other applicable data protection laws** is ensured.

5.3. Continuous Improvement

- Lessons learned from incidents, audits, and risk assessments are incorporated into security measures.
- The ISMS is continuously updated to **address emerging security threats**.

5.4. Cybersecurity Insurance

- AppTweak maintains a **Cyber Risk Insurance** policy to cover potential damages from security incidents.

6. Insurance

The Processor agrees to subscribe and maintain adequate liability insurance covering his various obligations.

Annex 2 - Sub-processing

The Processor is authorised to rely upon the following entities

(hereinafter: “Sub-processors”) in order to perform the following processing activities:

Sub-processors	**Location** (main establishment and location of data processing)	**Processing activities and description of the written agreement**
Amazon Web Services	Ireland	Data hosting

Linode	Germany	Data hosting
MongoDB	Ireland	Data hosting
Airbrake	United States	Bugg tracking software
Hubspot	EU	CRM
Intercom	EU	Customer support platform
Mailjet	United States	Email delivery service
Mixpanel	France	User tracking tool
Recurly	USA	Subscription management platform
Slack	United States	Chat communication tool
Hotjar	Ireland	User tracking tool
Gong	EU	Customer success call