APPFOLLOW

Know your apps — grow your business

Data Processing Agreement

This Data Processing Agreement ("**DPA**") is entered into between the Parties defined below and forms an integral part of the main agreement between the Parties, which governs the Customer's access to the Services and/or Consultancy Services provided by AppFollow ("**Agreement**"). This DPA shall apply with all its annexures when the Customer has engaged the Processor to process Personal Data on behalf of the Customer.

The effective date of this DPA is the same as that of the Agreement.

In case of discrepancies between the Agreement, the Privacy Policy and the DPA, this DPA and the Privacy Policy shall prevail.

1. Parties

1.1. _____ [**please insert official company name**], registered under the laws of _____ [**please insert country**] and having its registered office at _____ [**please insert registered address**] ("**Customer**")

and

1.2. **AppFollow.fi Oy**, registered under the laws of Finland and having its registered address at % Mikonkatu 9, 00100 Helsinki, Finland ("**Processor**").

1.3. The Customer and the Processor are also individually referred to as a "**Party**" and collectively as "**Parties**". For the purposes of this DPA, Customer is the controller as defined by the General Data Protection Regulation.

2. Definitions

2.1. The capitalized definitions used in this DPA shall be given the same meaning as in the Agreement, unless otherwise expressly stated in this DPA.

2.2. In addition, and for the purposes of this DPA, the following definitions shall apply:

a. "**Controller**" means the natural or legal person which determines the purposes and means of the processing of Personal Data. For the purposes of this DPA, the Controller means the Customer as defined in Section 1.1.;

b. "**Data Exporter**" means the Controller who transfers Personal Data, in this case the Customer;

c. "**Data Importer**" means the controller or processor who agrees to receive from the Customer Personal Data for further processing in accordance with this DPA, in this case the Processor;

d. "**Data Subject**" means identified or identifiable natural person who can be directly or indirectly identified, in particular by reference to an identifier such as a name, location data or an online identifier;

e. "**Data Protection Legislation**" means the General Data Protection Regulation (2016/679) and, to the extent applicable, the data protection or privacy laws of any other country applicable to either Party;

f. "**Personal Data**" means personal data relating to a Data Subject for which Customer is the Controller, and which is processed by the Processor on behalf of the Customer pursuant to or in connection with the Agreement;

g. "**Processor**" means the natural or legal person which processes Personal Data on behalf of the Controller. For the purposes of this DPA, the Processor means AppFollow.fi Oy as defined in Section 1.2.; and

h. "**Purpose**" means providing the Service/Consultancy Service, fulfilling the contractual obligations deriving from the Agreement and other reasons as may derive from the Agreement and/or other agreements which may be or become into force between the Parties;

3. Obligations of the Customer

3.1. The Customer undertakes and warrants that it is compliant with the provisions of applicable Data Protection Legislation regarding the Personal Data transferred to the Processor for processing purposes as set out in this DPA, including that the Personal Data has been, is and will be collected, processed, and transferred to the Processor in accordance with the Data Protection Legislation applicable to the Customer. The details of Personal Data are defined in Annex 1.

3.2. The Customer shall have sole responsibility for the accuracy, quality and legality of Personal Data and the means by which it acquired the Personal Data. The duties of the Customer include, but are not limited to:

a. establishing a procedure for the exercise of rights of such Data Subjects who Personal Data is collected;

b. only processing Personal Data that has been lawfully and validly collected; and

c. complying with data security and other obligations as set forth in Data Protection Legislation for controllers.

4. Processing Instructions

4.1. The Processor processes Personal Data on behalf of the Customer according to the Agreement and this DPA including their annexures and the applicable Data Protection Legislation, unless required to do so by law applicable to the Processor. This DPA and its annexures are deemed to constitute the Customer's written instructions to the Processor regarding processing of Personal Data.

4.2. Should this DPA be supplemented by additional annexures or instructions by request of the Customer, the Customer shall take reasonable steps and measures to ensure that instructions given to the Processor are legal. The Processor shall inform the Customer without delay if the Processor is of the opinion that an instruction by the Customer violates applicable provisions on data protection or this DPA. The Processor may suspend the implementation of the instruction in question until it has been confirmed to be according to applicable law or amended accordingly by the Customer in writing. The Processor may refuse to execute instructions that are obviously contrary to the Data Protection Legislation.

4.3. The Parties shall mutually nominate in writing one (1) or more contact persons for data protection matters. If there are changes in the contact persons, the Parties must inform each other of these in writing without undue delay.

5. Obligations of the Processor

5.1. The Processor shall retain, use, disclose and process Personal Data solely for the Purpose and in accordance with the terms of this DPA, unless otherwise required by applicable Data Protection Legislation. The Processor shall not sell Personal Data.

5.2. The Processor shall have and maintain appropriate technical and organizational measures to protect Personal Data against unauthorized, accidental, or unlawful loss, alteration, disclosure or access, and ensure that said measures provide a level of security appropriate to the risk caused by the processing, taking into account the nature of Personal Data being processed. The current technical and organizational measures are defined in Annex 2.

5.3. The Processor shall maintain strictest confidentiality regarding Personal Data and take reasonable steps to ensure the reliability of employees, agents, or contractors of both the Processor and any Subprocessors who may have access to Personal Data. The Processor shall ensure that persons authorized to process Personal Data in the name of (when employed by) the Processor are subjects of confidentiality undertakings regarding such Personal Data and/or are subject to a professional or statutory obligations of confidentiality.

5.4. The Processor shall provide assistance to the Customer by appropriate technical and organizational measures, insofar as this is possible and taking into account the nature of processing, for fulfilment of the Customer's obligation both to

a. respond to requests from Data Subjects regarding exercising rights granted to such Data Subjects by the Data Protection Legislation, namely Chapter III; and

b. demonstrate compliance with the duties of the Customer and the Processor.

5.5. The Processor shall, at the Customer's request and cost, provide assistance to the Customer where the Customer carries out a data protection impact assessment relating to Personal Data.

6. Third Party Sub Processors

6.1. The Processor may have the processing of Personal Data performed in whole or in part by other processors (hereinafter referred to as "**Subprocessor**"), which may be located outside the EU and/or the EEA.

6.2. The appointment of said Subcontractors by the Processor are hereby generally accepted by the Customer, which acceptance is subject to the following:

a. the Processor shall enter into a written contract with the Subprocessor;

b. the Processor shall ensure that the Subprocessor shall comply with obligations no less onerous than the Processor's obligations under this DPA; and

c. the Processor shall ensure that the Subprocessor is either located within the EU/the EEA or has given sufficient guarantees that it will provide at least the same level of protection for Personal Data as provided by the General Data Protection Regulation (including implementing appropriate technical and organizational measures), which can be done, for example, by way of implementing the standard contractual clauses as issued by the European Commission by decisions 2010/87/EU and 2001/497/EC as amended by 2004/915/EC .

6.3. Subcontracting as defined in this Section shall not release the Processor from its responsibility under this DPA. The Processor shall be liable for the acts and omissions of its Subprocessors to the extent the Processor would be liable if performing the processing itself.

6.4. In case there is a change in the Subcontractors appointed by the Processor, the Processor shall inform the Customer in writing and in advance of the appointment of a new Subcontractor or other changes in subcontracting. In case the Customer reasonably believes that said Subprocessor presents an unreasonable risk to Personal Data or prevents the Customer from complying with applicable data protection laws,

the Customer may, within thirty (30) days of receiving such notice from the Processor, notify the Processor that it objects to the Subprocessor and request the Processor to provide an alternative third party and/or on at least thirty (30) days' written notice to the Processor, terminate the Agreement and the DPA, in which case the Customer shall receive a pro rata refund of any fees paid in advance for the remainder of the applicable subscription period for the Service or Consultancy Service.

6.5. For the avoidance of doubt and for the purposes of this Section, subcontracting does not include services which the Processor uses as a purely ancillary service to support the Processor's business activities outside of providing the Service or Consultancy Service. However, the Processor is obliged to take appropriate precautions to ensure the protection of Personal Data, as necessary, also for such ancillary services.

7. Data Breaches

7.1. The Processor shall at its own cost inform the Customer without undue delay if the Processor becomes aware of any Personal Data breaches regarding Personal Data entrusted to the Processor by the Customer in respect of the Service or Consultancy Service.

7.2. For the purposes of this DPA, 'Personal Data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed by the Processor.

7.3. The notification shall:

a. describe the nature of the Personal Data breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

b. communicate the name and contact details of the contact point of the Processor where more information can be obtained, which can be the data protection officer or another employee or representative of the Processor;

c. describe the likely consequences of the Personal Data breach; and

d. describe the measures taken or proposed to be taken by the Processor to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.4. The Processor shall promptly initiate an investigation into the circumstances surrounding and resulting to the Personal Data breach, and immediately take the necessary measures to remedy the Personal Data breach as well as to mitigate possible adverse consequences, in particular for the persons concerned. In doing so the

Processor shall coordinate in good faith with the Customer. The Processor shall maintain records of Personal Data breaches, including remedial actions taken.

7.5. The Customer is responsible for communicating the Personal Data breach to the competent supervisory authority and, if the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons, to the Data Subject(s), unless otherwise agreed between the Parties in writing. The Processor shall provide assistance to the Customer for the purposes of said communication, taking into account the nature of processing and the information available to the Processor.

7.6. The Customer shall inform the Processor without delay if the Customer is of the opinion that there are errors in the processing by the Processor, or that the processing by the Processor violates applicable provisions of the Data Protection Legislation or this DPA.

8. Deleting or Returning Personal Data

8.1. The Processor shall cease processing Personal Data following termination or expiration of the Agreement (including permanently closing the Customer's Account(s)) and shall ensure that any Subprocessor shall similarly cease processing Personal Data.

8.2. Upon termination of the Agreement, the Processor shall on request transfer Personal Data back to the Customer, including all copies and back-ups.

8.3. Following termination or expiration of the Agreement and after receiving a written confirmation from the Customer, the Processor shall securely and irretrievably delete Personal Data, after which the Processor shall certify to the Customer that it has done so.

8.4. Notwithstanding the above, the Processor may retain Personal Data when required to do so under applicable Data Protection Legislation, in which case the processing of such Personal Data will be limited to the absolute minimum, and such Personal Data shall be deleted as soon as possible.

9. Rights of Data Subjects

9.1. If a Data Subject requests to use their rights pursuant to the General Data Protection Regulation Chapter III, the Processor shall provide the Customer reasonable assistance with the processing and handling of such request, taking into account the type of processing and the information that may be available.

9.2. In case a Data Subject submits such a request to the Processor instead of the Customer, the Processor shall, promptly upon becoming aware of such a request, inform the Customer thereof and the Parties shall promptly agree on action points together in good faith.

10. Audits

10.1. The Processor shall, upon a reasonable request to do so, provide the Customer with information needed by the Customer to demonstrate that the data processing by the Processor is in compliance with the terms of this DPA.

10.2. The Processor shall allow the Customer, or its authorized representatives selected by the Customer and not unreasonably objected by the Processor, to carry out audits to ascertain the Processor's compliance with the terms of this DPA, of which the Customer shall notify the Processor at least thirty (30) business days before performing the audit.

10.3. Any audits shall be carried out as efficiently as possible, during normal business hours and without disrupting business operations of the Processor. Any audits shall always take into consideration and maintain the Processor's obligations of confidentiality towards its other customers and/or other third parties.

10.4. In order to remedy the findings of an inspection, the Parties shall coordinate the measures to be implemented.

11. Damages

11.1. The liability for possible damages between the Parties shall be defined according to the General Data Protection Regulation Article 82.

11.2. The Processor shall compensate the Customer for direct damages incurred by the Customer due to an error or negligence by the Processor or its Subprocessor in processing Personal Data provided that the Processor has acted in breach of the Agreement and/or the terms of this DPA. Such compensation shall include requests for compensation by Data Subjects or the supervisory authority directed to the Processor and incurred directly due to breach of this DPA by the Processor.

12. Term and Termination

12.1. This DPA shall be in force until further notice, and shall terminate upon the fulfilment of both of the following conditions:

a. The Processor has returned or deleted Personal Data to the Customer in accordance with this DPA, namely Section 8; and

b. the Agreement between the Parties has been terminated, including permanently closing the Customer's Account(s).

12.2. Notwithstanding the above, the Parties mutually agree that the termination of this DPA, in any circumstances and for whatever reason, does not exempt them from the obligations and/or conditions of this DPA regarding Personal Data already transferred to the other Party.

13. Amendments

13.1. Any amendments or supplements to this DPA are to be agreed in writing, with explicit reference to this DPA and signed by an authorized representative of each Party in order for the amendment or supplement to be effective.

14. Governing Law

14.1. This DPA and any dispute or claim arising out of or in connection with it or its subject matter shall be governed by, and construed in accordance with, Finnish law pursuant to the jurisdiction of Finnish courts.

The Parties have duly executed this DPA as of _____.

On behalf of the Processor	On behalf of the Customer
_____	_____
Name: Evgeny Kruglov	Name:
Title: COO, co-founder	Title:
Company: AppFollow.fi Oy	Company:

Annex 1
Subject Matter and Details of Data Processing

Subject Matter
The Processor's provision of the Service and/or Consultancy Service to the Customer.

Duration of the Processing
The term according to Section 12 of the DPA, added with the period from the expiry of the said term until deletion of all Personal Data by the Processor in accordance with the DPA or a legal obligation as according to applicable Data Protection Legislation.

Nature and Purpose of the Processing
The Processor will process Personal Data for the purposes of providing the Service and/or Consultancy Service in accordance with the DPA.

Type of Personal Data Processed
Data regarding individuals who have published reviews for Apps to publicly available Application Stores, as selected by the Customer, namely the following:

a. names or nicknames of the reviewers of Apps chosen by the Customer (may be actual names or nicknames as chosen by each reviewer);
b. information included in the body texts of such reviews;
c. geographical location (country);
d. language of the review;
e. OS version; and
f. in case of Google Play, device details, subject to the reviewer connecting necessary integrations.

Categories of Data Subjects
Individuals who have published reviews for Apps to publicly available Application Stores, as selected by the Customer.

Current Subprocessors used for processing of Personal Data
The Processor currently uses the following Subprocessors for storage of Personal Data. Besides storage, no other processing tasks of Personal Data have been outsourced to Subprocessors.

Subprocessor	**Subprocessing activity**	**Location of data**
Amazon AWS	Storage of data necessary to provide the Service or Consultancy Service	Germany
Hetzner Online GmbH and Hetzner Finland Oy	Storage of data necessary to provide the Service or Consultancy Service	Finland, Germany

Annex 2
Security Measures of the Processor

The Processor is entitled to update and change the measures described in this Annex 2 in the future, subject to that the level of protection granted for Personal Data is not significantly or materially lessened and that the measures continue to be compliant with the Data Protection Legislation. A prior written consent of the Customer shall be acquired before implementing any material or significant changes.

1. Physical access control

   AppFollow uses two types of partitions for customers on server level and app level based on database records. AppFollow has permissions for each customer via our application logic.

2. Access restriction mechanisms

   Customers have three options for acquiring access to their Account for the Service: login/pass, Open Authorization (available via Google, Slack or Linkedin) or Single sign-on (SSO).

   Hashicorp vault (provided by HashiCorp, Inc.) is used for management of sensitive information, such as keys, tokens, and passwords.

   Some parts of AppFollow Services utilize role-based access control (RBAC), meaning that some employees have access to Customer's data via Multi-factor authorization (MFA). Said access is granted based on employees' job function on a need-to-know basis. AppFollow has a log activity system in place, in addition to which all employees are required to sign an adequate non-disclosure agreement and undergo training about privacy and data protection.

   Further, firewalls have been set up for AppFollow's servers.

3. Data access control

   AppFollow has assigned different roles and thus grants different permissions for specific employees based on their work tasks in AppFollow's admin panel via MFA.

4. Communication and transport control

   AppFollow uses Virtual Private Network (VPN) and Hypertext Transfer Protocol Secure (HTTPS) to ensure that data cannot be read, copied, modified, or deleted without authorization during electronic transmission.

Sensitive data is encrypted by using Advanced Encryption Standard (AES) 256.

5. Entry control

AppFollow has and maintains a log activity system which is monitored and controlled at regular, weekly intervals.

6. Processing control

For data storage, AppFollow uses only such Subprocessors, with which AppFollow has a written DPA and which have provided appropriate guarantees/safeguards (such as SCCs) that the level of data protection granted by such Subprocessor is the same as the level defined in the General Data Protection Regulation.

Regarding Personal Data, the Controller of which is the Customer, AppFollow only uses Subprocessors for data storage purposes, meaning no other processing tasks are outsourced to Subprocessors.

7. Availability control

AppFollow monitors all of its infrastructure with Pingdom (provided by SolarWinds Worldwide, LLC). Monitoring is targeted to specific test accounts created for this purpose, meaning the third-party providing monitoring services has no access to Personal Data. In addition, AppFollow conducts regular backups to be able to restore data in case of a physical or technical incident and to protect said data against accidental destruction or loss.

8. Separation control

In order to ensure that the collected data can be processed separately for different purposes, AppFollow utilizes an architecture based on micro-services and restricts the access granted to employees to access data based on job functions of each employee.

9. Continued Evaluation

AppFollow strives to develop and improve the security of our Service and Consultancy Service.

We follow Open Web Application Security Project (OWASP) to acquire knowledge of the latest tools and technologies in the field of web application security.

We also use an independent third-party, SonarQube (provided by SonarSource S.A), for static code analysis to identify potential vulnerabilities and to be able to promptly act on them.

Further, we conduct penetration tests at least annually by an independent third-party provider, HackerOne, Inc., to learn about points for improvements and quickly act on the same. The latest penetration test was completed in April/May 2021.