APPFOLLOW

Know your apps – grow your business

DATA PROCESSING AGREEMENT

Public offer — AppFollow

1. Introduction and Acceptance

This Data Processing Agreement ("DPA") is a public offer made by the applicable AppFollow contracting entity — AppFollow.fi Oy (Bulevardi 21, 00100 Helsinki, Finland) for customers in the EEA/UK, or AppFollow, Inc. (c/o Nordic Innovation House, 470 Ramona Street, Palo Alto, CA 94301, USA) otherwise (the "Processor" or "AppFollow") — to any customer that uses AppFollow's services (the "Customer").

This DPA forms an integral part of, and is incorporated by reference into, the agreement between the Parties governing the Customer's access to the Services and/or Consultancy Services provided by AppFollow (the "Agreement"), including any Order Form and the AppFollow Terms and Conditions.

By accepting an AppFollow Order Form, by agreeing to the AppFollow Terms and Conditions, or by otherwise using the Services, the Customer accepts this DPA and is deemed to have entered into it with AppFollow. No separate signature is required for this DPA to be legally binding. It applies whenever AppFollow processes Personal Data on the Customer's behalf, and its effective date is the same as that of the Agreement.

The Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Legislation, its affiliates for whom AppFollow processes Personal Data. The identity and details of the Customer are those set out in the Agreement and the applicable Order Form.

In case of conflict, the order of precedence is: (1) the Standard Contractual Clauses referenced in the International data transfers section; (2) this DPA; and (4) the Agreement. The Customer and AppFollow are each a "Party" and together the "Parties".

2. Roles and Scope of Processing

This DPA applies solely to Personal Data processed by the Processor on behalf of the Customer in connection with the provision of the Services (the App Store Review Data and Customer Authorised User Data described in Annex 1) ("**Processor Data**"). In respect of Processor Data, the Customer is the Controller and AppFollow is the processor.

The Parties acknowledge that the Processor also processes certain Personal Data as an independent Controller, including, without limitation:

- business contact details of the Customer's commercial, legal, administrative and billing representatives;
- information necessary for entering into, administering and performing the Agreement;
- billing and payment information;
- customer support communications;
- information processed for security, fraud prevention, legal compliance and operation of the .

Such processing is carried out by the Processor in its capacity as an independent Controller, is governed by the Processor's Privacy Policy and applicable Data Protection Legislation, and does not fall within the

scope of this DPA. Each Party acts as an independent Controller in respect of such data and is individually responsible for its own compliance; nothing in this DPA constitutes the Parties as joint controllers.

3. Definitions

Capitalised terms not defined here have the meaning given in the Agreement. "**Data Protection Legislation**" means Regulation (EU) 2016/679 ("**GDPR**") and any other applicable data protection or privacy laws. "**Personal Data**" for the purposes of this DPA means Processor Data — personal data processed by the Processor on behalf of the Customer under the Agreement, as described in Annex 1. "**SCCs**" means the standard contractual clauses approved by the European Commission by Implementing Decision (EU) 2021/914 of 4 June 2021. Other terms ("controller", "processor", "Data Subject", "processing") have the meaning given in the GDPR.

4. Obligations of the Customer

The Customer warrants that Personal Data has been and will be collected, processed and transferred to the Processor in compliance with applicable Data Protection Legislation, and that it has all necessary rights, consents and legal bases to do so. The Customer is solely responsible for the accuracy, quality and legality of the Personal Data and for establishing procedures for Data Subjects to exercise their rights, including informing its authorised users and other relevant Data Subjects of the processing.

5. Processing Instructions

The Processor processes Personal Data only on the Customer's documented instructions (of which this DPA and its annexes form part) and for the purpose of providing the Services, unless required otherwise by applicable law. The Processor will inform the Customer without undue delay if, in its opinion, an instruction infringes Data Protection Legislation. Each Party's contact point for data protection matters is set out in the Contact section below.

6. Obligations of the Processor

- The Processor shall process Personal Data solely for the purpose of providing the Services and in accordance with this DPA, and shall not sell Personal Data.
- The Processor shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in **Annex 2**.
- The Processor shall ensure that persons authorised to process Personal Data are bound by appropriate confidentiality obligations, and shall take reasonable steps to ensure the reliability of such personnel and of any Subprocessor's personnel.
- Taking into account the nature of the processing and the information available to it, the Processor shall provide reasonable assistance to the Customer, by appropriate technical and organisational measures where appropriate, to enable the Customer to comply with its obligations under Articles 32 to 36 of the GDPR, including in relation to Data Subject requests, security of processing, Personal Data breaches, data protection impact assessments and prior consultations with supervisory authorities.

7. Third-Party Subprocessors

The Customer provides a general authorisation for the Processor to engage subprocessors (each a "**Subprocessor**"), which may be located outside the EU/EEA, to process Personal Data in connection with the Services. The current list of authorised Subprocessors — including their subprocessing activity,

location and applicable transfer safeguards, and any AI-related Subprocessors engaged for optional AI-powered functionality — is maintained at the AppFollow Trust Center: AppFollow Trust Center.

The Processor shall impose on each Subprocessor, by written contract, data protection obligations no less onerous than those in this DPA, and shall ensure the Subprocessor is either located in the EU/EEA or provides adequate safeguards (including the SCCs where required). The Processor remains liable for the acts and omissions of its Subprocessors as if performed by the Processor itself.

The Processor shall notify the Customer of any intended addition or replacement of a Subprocessor at least thirty (30) days before the new Subprocessor begins processing Personal Data. Notice shall be given by email to the Customer's contact identified on the cover sheet (or, where no contact is identified, to the Customer's account administrator email) and by updating the Subprocessor list at the AppFollow Trust Center. The Customer is responsible for keeping its notice contact details up to date.

The Customer may object to the intended change on reasonable data-protection grounds by written notice within thirty (30) days of the Processor's notice. The Parties will work in good faith to resolve the objection; if it cannot be resolved within thirty (30) days, the Customer may, as its sole remedy, terminate the affected Services by written notice and receive a pro rata refund of prepaid fees for the remaining subscription period. If the Customer does not object within the objection period, the change is deemed approved.

Purely ancillary services supporting the Processor's business (and not the provision of the Services) are not subprocessing, but the Processor shall nonetheless take appropriate precautions to protect Personal Data.

8. International Data Transfers

The Customer acknowledges that the Processor may transfer and process Personal Data in the United States and elsewhere where the Processor, its affiliates or its Subprocessors operate. The Processor shall ensure such transfers comply with Data Protection Legislation.

Where the Processor receives Personal Data protected by the GDPR ("**EU Data**") in a country not benefiting from a European Commission adequacy decision, the SCCs apply and are hereby incorporated into this DPA by reference and deemed entered into by the Parties. The Processor is the "data importer" and the Customer is the "data exporter". The SCCs are completed as set out in Section 7.3, using the information in **Annex 1** (Annex I and III of the SCCs) and **Annex 2** (Annex II of the SCCs). The full text of the SCCs, as published by the European Commission, is available at eur-lex.europa.eu and prevails in case of conflict with this DPA.

7.3 SCC options. For the incorporated SCCs the Parties agree:

- Module Two (Controller to Processor) applies where the Customer is a controller; Module Three (Processor to Subprocessor) applies where the Customer is a processor acting on behalf of a third-party controller;
- Clause 7 (optional docking clause) does not apply;
- in Clause 9, Option 2 (general written authorisation) applies, with the notice period set out in Section 6;
- the optional wording in Clause 11 does not apply;
- for the purposes of Clause 17, the governing law shall be the laws of Finland; and
- for the purposes of Clause 18(b), disputes are resolved before the courts of Finland; the competent supervisory authority is identified in Annex 1.

If the Processor adopts an alternative lawful transfer mechanism, or if a competent authority rules that the mechanism above cannot be relied on, the Processor may implement any additional safeguards reasonably required to enable the lawful transfer of EU Data, and that mechanism shall apply instead to the extent it complies with the GDPR.

UK transfers. Where the Processor receives Personal Data protected by the UK GDPR and the Data Protection Act 2018 ("UK Data") in a country not covered by UK adequacy regulations, the Parties agree that the SCCs shall apply as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0) issued by the UK Information Commissioner under s.119A of the Data Protection Act 2018 ("UK Addendum"), which is hereby incorporated into this DPA by reference. For the purposes of the UK Addendum: Table 1 is completed with the Parties' details on the cover sheet; Table 2 refers to the SCCs as completed in Section 7.3; Table 3 refers to Annexes 1 and 2 of this DPA; and for Table 4, neither Party may end the UK Addendum as set out in Section 19 of the UK Addendum. References in the SCCs to the GDPR shall, in respect of UK Data, be read as references to the UK GDPR, the competent supervisory authority shall be the UK Information Commissioner, and Clauses 17 and 18 shall be read as referring to the laws and courts of England and Wales.

Swiss transfers. Where the Processor receives Personal Data protected by the Swiss Federal Act on Data Protection ("FADP") ("Swiss Data") in a country not benefiting from an adequacy decision of the Swiss Federal Council, the SCCs shall apply as adapted as follows: (a) references to the GDPR shall be read as references to the FADP; (b) the competent supervisory authority under Clause 13 shall be the Swiss Federal Data Protection and Information Commissioner (FDPIC); (c) references to "Member State" shall be interpreted so as not to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence; and (d) the term "personal data" shall include data relating to legal entities to the extent (if any) such data is protected under the FADP. Clauses 17 and 18 of the SCCs remain as set out in Section 7.3, without prejudice to mandatory Swiss law.

9. Personal Data Breaches

The Processor shall, at its own cost, notify the Customer without undue delay, and in any event no later than seventy-two (72) hours, after becoming aware of a Personal Data breach affecting the Customer's Personal Data. The notification shall describe, to the extent available, the nature of the breach (including the categories and approximate numbers of Data Subjects and records concerned), a contact point, the likely consequences, and the measures taken or proposed to address and mitigate it. Where it is not possible to provide all such information at once, it may be provided in phases without further undue delay.

The Processor shall investigate the breach, take necessary remedial and mitigating measures, coordinate in good faith with the Customer, and maintain records of breaches and remedial actions. The Customer is responsible for any notification to supervisory authorities (which the Customer must generally make within 72 hours of becoming aware, in accordance with Article 33 GDPR) and to Data Subjects, and the Processor shall provide reasonable assistance taking into account the nature of processing and the information available to it.

10. Deletion or Return of Personal Data

On termination or expiry of the Agreement the Processor shall cease processing Personal Data and ensure Subprocessors do the same. At the Customer's choice, the Processor shall return Personal Data (including copies and back-ups) or, on the Customer's written confirmation, securely and irretrievably delete it and certify deletion. The Processor may retain Personal Data where required by applicable law, limited to the minimum necessary and deleted as soon as possible thereafter.

11. Rights of Data Subjects

The Processor shall provide reasonable assistance to the Customer in handling Data Subject requests under Chapter III of the GDPR. If a Data Subject contacts the Processor directly, the Processor shall promptly inform the Customer and the Parties shall agree next steps in good faith; the Processor shall not respond without the Customer's authorisation, except to redirect the request to the Customer.

12. Audits

On reasonable written request, the Processor shall make available information necessary to demonstrate compliance with this DPA. Such information may be provided through the Processor's certifications, audit reports and security documentation (including ISO certificates, independent audit reports, penetration testing summaries and similar documentation) available at the AppFollow Trust Center (Trust Center). Where that documentation is insufficient to demonstrate compliance, the Customer (or an auditor it appoints and to which the Processor does not reasonably object) may conduct an audit on at least thirty (30) business days' written notice, no more than once per year, during normal business hours, in a manner that minimises disruption and preserves the Processor's confidentiality obligations to third parties. The Parties shall coordinate on measures to remedy any findings.

13. Liability

Liability between the Parties is determined in accordance with Article 82 GDPR and subject to the limitations of liability in the Agreement, except to the extent prohibited by applicable Data Protection Legislation. The Processor shall compensate the Customer for direct damages caused by the Processor's or its Subprocessor's breach of this DPA in processing Personal Data, including claims by Data Subjects or supervisory authorities arising directly from such breach.

14. Term, Termination and Amendments

This DPA remains in force until the Agreement has terminated and the Processor has returned or deleted Personal Data in accordance with Section 9. Termination of this DPA does not relieve either Party of obligations concerning Personal Data already processed.

As this DPA is provided as a public offer incorporated into the Agreement, the Processor may update it from time to time; any material change will be notified through the Services, the AppFollow website or other reasonable means, and continued use of the Services after the update takes effect constitutes acceptance of the updated DPA. Updates that materially reduce the protection afforded to Personal Data will not apply retroactively.

15. Governing Law

This DPA is governed by the laws of Finland and subject to the jurisdiction of the Finnish courts, without prejudice to the governing law of the SCCs under Section 7.3.

16. Contact Details

The Processor's contact point for data protection matters and notices under this DPA is the AppFollow Privacy Team, legal@appfollow.io. The Customer's contact point is the individual or role identified in the Agreement or Order Form, or otherwise the Customer's primary account administrator. Each Party shall keep its contact details current; a change of contact details does not constitute an amendment to this DPA.

Signed (Bilateral) Version

This DPA is legally binding through acceptance of the Agreement and does not require signature. However, if the Customer requires a separate, counter-signed bilateral DPA, the Customer may download the AppFollow bilateral DPA template at appfollow.io/legal/dpa-template, complete the required details, and send the completed document for review and signature to the AppFollow legal team at legal@appfollow.io. A bilateral DPA becomes binding only once counter-signed by an authorised representative of AppFollow. Unless and until a bilateral DPA is executed, this public-offer DPA governs the processing of Personal Data.

Annex 1 — Subject matter and details of data processing

This Annex sets out the details of the processing and provides the information required by Annex I to the SCCs.

Subject matter	The Processor's provision of the Services and/or Consultancy Services to the Customer.
Nature and purpose	Processing of Personal Data for the purpose of providing the Services and/or Consultancy Services in accordance with this DPA and Contract between the parties.
Duration	The term of the Agreement, plus the period until deletion of all Personal Data under Section 9 or as required by applicable law.
Frequency of transfer	Continuous.
Categories of Data Subjects	Individuals who have published reviews for applications on publicly available app stores, as selected by the Customer.
Retention period	Until termination or expiry of the Agreement, subject to Section 9.
Subprocessors	The current list of Subprocessors — including subprocessing activity, location, transfer safeguards and any AI-related Subprocessors — is maintained at the AppFollow Trust Center. Subprocessors process Personal Data for the duration of the Agreement. The Processor may update the list from time to time in accordance with Section 6.3.
Competent supervisory authority	As identified on the cover sheet: the supervisory authority of the EU/EEA Member State determined in accordance with Clause 13 of the SCCs (by reference to the Customer as data exporter). Where AppFollow.fi Oy is the contracting entity, this is the Finnish Data Protection Ombudsman / Tietosuojavaltuutettu.

Types of Personal Data

Data Set A — App Store review data

Source: Publicly available app stores, for applications selected by the Customer. Categories of Data Subjects: Individuals who have published reviews for such applications.

Data category	Description
Reviewer information	Publicly available app review information, including reviewer identifiers (where available), review content, language and country.
Technical metadata	Technical information associated with the review, including operating system version and, where supported by the relevant app store (e.g. Google Play), device information.

Data Set B — Customer authorised user data

Source: Provided by the Customer through the administration and use of the Services, including user provisioning and account management within the Service.

Categories of Data Subjects: The Customer's employees, personnel and other individuals whom the Customer authorises to access or administer the Service ("authorised users").

Data category	Description
Identity	Full name of the authorised user.

Contact data	Business email address.
Professional data	Job title / role within the Customer's organisation.
Account data	Data generated in connection with account set-up, access management and use of the Service's administration panel (e.g. user account and permission records).

Sensitive data

No special-category data (Article 9 GDPR) is solicited or required for either data set. Such data may only occur incidentally in Data Set A if a reviewer unexpectedly includes it in unstructured review text; it is not intended to be transferred.

Optional AI Processing

Where the Customer elects to use optional AI-powered functionality made available as part of the Services, Personal Data may be processed by the Processor's authorised AI Subprocessor solely for the purpose of providing such functionality (including, for example, review analysis, summarisation and response generation).

AI processing is limited to publicly available app store reviews and related customer-created review tags required for the requested functionality. The Processor applies data minimisation principles and submits only the minimum information necessary to provide the relevant AI functionality. Data processed through such AI functionality is not used to train or improve the AI provider's models, and zero data retention is applied where supported by the AI Subprocessor.

AI processing is optional and takes place only where the Customer enables and uses the relevant AI functionality.

Annex 2 — Technical and organisational security measures

The Processor maintains and continuously reviews a documented information security programme designed to ensure a level of security appropriate to the risks associated with the processing of Personal Data, taking into account the nature, scope, context and purposes of the processing.

The Processor's technical and organisational measures include, among others:

(1) identity and access management, including role-based access controls and multi-factor authentication where appropriate;
(2) authentication, password and credential management;
(3) encryption of Personal Data in transit and at rest, where appropriate;
(4) network, infrastructure and endpoint security measures;
(5) secure software development and vulnerability management processes;
(6) logging, monitoring and security event management;
(7) business continuity, disaster recovery and backup procedures;
(8) incident detection, response and Personal Data breach management;
(9) personnel security, confidentiality obligations and regular security awareness training;
(10) vendor and subprocessor security management; and
(11) periodic security assessments, vulnerability management, penetration testing and continuous improvement of security controls.

The Processor may update these technical and organisational measures from time to time, provided that such updates do not materially reduce the overall level of protection afforded to Personal Data.

A current and more detailed description of the Processor's technical and organisational measures, together with information regarding the Processor's applicable security certifications, independent audit reports, the latest penetration testing summary and other relevant security documentation, is maintained at the AppFollow Trust Center and is incorporated into this DPA (including Annex II to the SCCs) by reference.

The AppFollow Trust Center is available at: AppFollow Trust Center.