Filestash

Data Processing Agreement

Summary

Concluded by and between [Customer] (hereinafter "Controller") and Filestash Pty Ltd., a company incorporated under the laws of Australia, with its registered offices in Australia and address 20 Herbert street, 2114 West Ryde, with company number 88 666 528 187 (hereinafter "Processor") (Controller and Processor together hereinafter "Parties" and each hereinafter "Party") on the processing of personal data on behalf of Controller by Processor.

Contents

1 Preamble

This Data Processing Agreement, (hereinafter "DPA") outlines the Parties' obligations in respect of protecting personal data, associated with the processing of such data on behalf of the Controller by the Processor as set out in the Processor's subscription terms accepted/subscribed to by the Controller (hereinafter "Subscription / Subscription Terms").

This DPA is supplemental to, and constitutes an integral part of, the Subscription / Subscription Terms or any other contract entered into with the Processor, and becomes effective upon the Controller's acceptance of the Subscription / Subscription Terms or execution of another agreement with the Processor.

Throughout this DPA, any reference to "Data Protection Laws" refers, where applicable, to the FADP, the GDPR, the UK GDPR, and any subsequent data-protection statutes or regulations in effect in the jurisdiction(s) where the Processor is established and/or conducts processing activities.

2 Scope and specification of personal data processing

2.1. The purpose of the Processor's processing activity is to provide the Controller with the subscribed access to and use of the Processor's software, either through a web browser or programmatically through its public API (hereinafter "Services").

2.2. Within this DPA's scope, the following categories of personal data may be processed: Company or organization name, first name(s), middle name(s) and last name(s) (as applicable), past and current position(s) represented by role(s) the employee holds, e-mail addresses, IP addresses (anonymized), cookies used for authentication, cookies tracking user behaviour (global opt-out, anonymized) solely to identify product-usability issues, operating system version, browser version, usernames, passwords (encrypted), access logs, geolocation indicators, photographic or illustrative imagery, credit-card details (for subscription purchases made with a card), bank details, account number or work address (for subscription purchases via invoice). Furthermore, any

content copied, pasted or uploaded by the data subjects defined in clause 2.3 below.

2.3. Within this DPA's scope, the following categories of the Controller's data subjects may be processed, depending on the documents uploaded: customers, employees, suppliers, business partners of the Controller, as well as any other persons whose personal data appears in documents uploaded by the Controller.

3 Duration of DPA and obligations after termination

3.1. The duration of this DPA is subject to the Subscription / Subscription Terms.

3.2. Upon expiry of the product's subscription period, the Processor undertakes to delete or destroy all personal data of the Controller held by it in accordance with data protection requirements and/or return to the Controller all personal data and data carriers provided to it under the Subscription / Subscription Terms. Deletion or destruction will occur unless a legal obligation requires retention. If law mandates retaining certain personal data for a set period, the Processor will maintain it for that duration and then delete or destroy the data in line with Data Protection Laws.

4 Controller's rights and obligations

4.1. The Processor handles personal data on behalf of the Controller in accordance with the Controller's instructions. The instructions set out in this DPA, the Subscription / Subscription Terms and any directions issued by the Controller via the configuration options within the Services shall be deemed the authorised instructions for the purposes of this DPA. Additional instructions may only be provided where the Parties have mutually agreed in writing or in another documented electronic form (e.g., via email).

4.2. Changes to the subject matter of the processing or to any procedures shall be coordinated between the Controller and the Processor and recorded

in writing or another documented electronic form.

4.3. The Controller shall bear sole responsibility for the lawfulness of disclosing personal data to the Processor and for having such personal data processed on its behalf. The Controller is the "controller" as defined in Article 5 lit. j FADP and Article 4 no. 7 GDPR and UK GDPR.

4.4. Subject to clause 4.5 of this DPA, the Controller alone is responsible for addressing data-subject rights requests. If a data subject asserts a claim for rectification, erasure or access against the Processor, the Processor shall promptly forward the claim to the Controller and assist the Controller where reasonably possible.

5 Processor's rights and obligations

5.1. The Processor shall process (collect, store, retain, use, modify, disclose, archive, delete or destroy, etc.) personal data solely as set out in this DPA, the Subscription / Subscription Terms, and in accordance with the Controller's instructions.

5.2. The Processor may not delete or destroy personal data on its own initiative; any such deletion or destruction must be carried out only on a written instruction from the Controller, unless a legal requirement compels otherwise.

5.3. The Processor undertakes to treat all personal data processed under this DPA as confidential. This confidentiality obligation continues to apply after termination of this DPA. The Processor will ensure that everyone granted access to the personal data or contracted to process it is made aware of this duty and is contractually bound to it. The Processor will also maintain appropriate internal organisational measures—such as staff training in Data Protection Laws and strict access controls—to guarantee that only authorised personnel can access personal data.

5.4. At the Controller's direction, the Processor shall correct any personal data found to be inaccurate or incomplete. If a data subject asserts their rights (for information, access, rectification, erasure, objection, or data portability) directly against the Processor, the Processor shall promptly direct the data subject to the Controller and await further instructions.

5.5. The Processor shall use reasonable efforts to assist the Controller in fulfilling data-subject rights under applicable law and in meeting the Controller's legal obligations, taking into account the nature of the processing and the information available to the Processor. The Controller will reimburse the Processor for any reasonable additional costs incurred in providing such assistance.

5.6. The Processor may use the Controller's personal data for pattern recognition, trend analysis, and predictive or recommendation analytics, provided the data is irreversibly anonymised so that it cannot be re-linked to any individual.

5.7. The Processor may use the Controller's company name on Filestash's website and in marketing materials referring to Filestash customers. The Controller may opt out of such mentions at any time by emailing support@filestash.app.

5.8. The Processor shall promptly notify the Controller if it becomes aware of an infrigement or if any instruction received from the Controller appears to conflict with applicable Data Protection Laws.

6 Information and audit rights

6.1. At the Controller's request, the Processor shall give the Controller with all information reasonably necessary to demonstrate compliance with the Processor's obligations, including details of the technical and organisational measures implemented.

6.2. The Processor shall supply the Controller with suitable evidence of compliance, such as self-audit reports, attestations, certifications, audit extracts from independent bodies (e.g., external auditors), or other appropriate documentation.

6.3. If the Controller has reasonable doubts about the documents provided by the Processor under clause 6.2 and conveys those doubts to the Processor, the Controller or a reputable third-party auditor appointed by the Controller may verify the Processor's compliance with clause 6.1. Such an inspection is subject to the conclusion of a market-standard non-disclosure agreement.

6.4. The Controller shall promptly inform the Processor of any errors or irregularities discovered during the audit.

6.5. The Controller shall bear any additional costs incurred by the Processor in connection with the audit under clauses 6.3 and 6.4, unless the audit reveals that the Processor has breached this DPA or applicable Data Protection Laws.

7 Sub-processor

7.1. The Controller hereby authorizes the Processor to engage sub-processors to fulfil its obligations under the Subscription / Subscription Terms.

7.2. Current sub-processors are listed in Annex 2 of the DPA.

7.3. Before engaging any new or replacement sub-processor, the Processor shall inform the Controller and allow a 14-day period for the Controller to object on data-protection grounds. If the Controller does not object within that time, consent is deemed given. Should the Controller object, the Processor will not grant that sub-processor access to the Controller's personal data.

7.4. The Processor shall ensure, via an agreement with each sub-processor, that such sub-processor assumes obligations no less protective than those the Processor has under this DPA.

7.5. The Processor remains fully liable to the Controller for all acts and omissions of its sub-processors.

8 Processing locations

8.1. Processing of personal data is carried out exclusively in Australia, the European Union, and by certain sub-processors in designated third countries. Where the Processor's personnel require service provision during holiday absences or from a temporary remote-work site, the Controller exceptionally authorises the Processor to handle data from such abroad locations via secure remote access, protected by strong passwords, encrypted connections and use

of the Processor's own device, which is protected against third-party access.

8.2. For sub-processors located in third countries, the Processor ensures an equivalent level of data protection by adopting standard contractual clauses pre-approved or recognised by the relevant data-protection authorities.

9 Technical and organizational measures

9.1. The Processor applies appropriate technical and organisational measures under Articles 7 and 8 FADP or Article 32 GDPR/UK GDPR to safeguard personal data against unauthorised access, loss or destruction. This includes firewalls, state of the art encryption technologies, access controls and other safeguards listed in Annex 1.

9.2. These technical and organisational measures are periodically reviewed and updated as needed to remain aligned with current technological best practices and applicable data protection requirements.

10 Warranties

The Processor warrants that:

- it will comply with all applicable Data Protection Laws when providing the Services and processing any personal data;
- it will adhere to any requirements under Data Protection Laws concerning data impact assessments and directives issued by competent supervisory authorities or regulators; and
- it will inform the Controller of any data protection breach without undue delay and, in any event, no later than 72 hours after becoming aware of the breach.

11 Liability

The Controller shall be liable to data subjects for damages or other claims arising from the processing of personal data that directly results from the Controller's breach of Data Protection Laws or this DPA. Direct claims against the Processor are permitted only if the Processor has itself violated this DPA or the applicable Data Protection Laws.

12 Final provisions

12.1. If any provision of this DPA conflicts with the Subscription / Subscription Terms or any other agreement between the Parties, the terms of this DPA shall prevail.

12.2. Changes or additions to this DPA require the mutual consent of both Parties and must be signed by an authorised representative of each Party, subject to Section 13.3 below.

12.3. Annex 1 and Annex 2 are integral parts of this DPA. The Processor may update Annex 2 (to add or replace sub-processors) in accordance with Section 7.3. The technical and organisational measures in Annex 1 may be substituted at any time by measures of equal or greater effectiveness, provided the Processor gives the Controller at least 30 days' prior notice.

12.4. This DPA is governed by the substantive laws of Australia, to the exclusion of the conflict of laws rules and international treaties. The Place of jurisdiction shall be with the state courts at the Processor's registered office.