

Data Processing Agreement

Accolade Software Products LLC · c/o Harvard Business Services, Inc., 16192 Coastal Hwy, Lewes, DE 19958, United States · sales@cmcfy.com · Version of 1 November 2026 · cmcfy.com/dpa

Draft pending legal review. This agreement is a draft and has not yet been reviewed by a lawyer. It describes how CMCfy works today. Last updated 1 November 2026.

This Data Processing Agreement ("DPA") forms part of the agreement under which Accolade Software Products LLC ("CMCfy", "we") provides CMCfy to a business customer ("Customer"): the [Terms of Use](#) together with any order, plan or signed contract (the "Agreement"). It applies when CMCfy processes personal data on the Customer's behalf. The Customer can accept it by signing the PDF copy, or it applies automatically when the Customer's order refers to it. Where this DPA and the Agreement differ on personal data, this DPA wins; where this DPA and the Standard Contractual Clauses differ, the Clauses win.

1. How CMCfy is built, and why so little is processed

The CMCfy tools run in the Customer's browser. Files, data, projects, audit trails and reports stay on the Customer's computers or in a folder the Customer picks, and CMCfy never receives them. CMCfy therefore processes Customer personal data only in the limited cases in Annex I: user accounts, usage counts, support correspondence, and the text a user chooses to send with CMCfy Writer, which passes through our server to the writing service and is not stored by us.

2. Roles and definitions

For the processing in Annex I, the Customer is the controller and CMCfy is the processor (or, where the Customer is itself a processor, CMCfy is its subprocessor). Terms such as "personal data", "processing", "controller", "processor", "data subject" and "personal data breach" have the meanings in the GDPR (Regulation (EU) 2016/679), the UK GDPR, or the other data protection laws that apply ("Data Protection Law"). For US state laws such as the California Consumer Privacy Act, CMCfy acts as the Customer's "service provider" or "processor". CMCfy processes its own business data (for example billing records and its own marketing contacts) as a controller under its [Privacy Policy](#), not under this DPA.

3. CMCfy's obligations

- **Instructions.** CMCfy processes Customer personal data only to provide CMCfy under the Agreement and on the Customer's documented instructions, which are the Agreement, this DPA and the Customer's use of the product settings. CMCfy will tell the Customer if it believes an instruction breaks Data Protection Law. If the law requires other processing, CMCfy will tell the Customer first unless the law forbids it.
- **US state laws.** CMCfy will not sell or share Customer personal data, use it for any purpose outside the Agreement, combine it with personal data from other sources except as the law allows a service provider to, or keep, use or disclose it outside the direct business relationship with the Customer. CMCfy will tell the Customer if it can no longer meet these obligations.
- **Confidentiality.** Everyone CMCfy authorises to process Customer personal data is bound by confidentiality.
- **Security.** CMCfy keeps the technical and organisational measures in Annex II in place, and may improve them but will not lower the overall level of protection.
- **Help with requests.** Taking into account that CMCfy holds very little, CMCfy will help the Customer answer data subjects' requests, and with security, breach notification, data protection impact assessments and

consultations with authorities. If a data subject contacts CMCfy directly about Customer personal data, CMCfy will pass the request to the Customer and not answer it alone unless the Customer asks.

- **Breaches.** CMCfy will notify the Customer without undue delay, and in any case within 72 hours, after becoming aware of a personal data breach affecting Customer personal data. The notice will describe what happened, the data and people affected as far as known, the likely consequences, what CMCfy is doing about it and a contact. CMCfy will update the Customer as it learns more.
- **Deletion.** When the Agreement ends, CMCfy will delete Customer personal data within 90 days, unless the law requires it to keep some of it, in which case it stays protected by this DPA. Writing text is never stored, so there is nothing to return. The Customer's own files stay with the Customer throughout.
- **Audits.** CMCfy will make available the information needed to show it meets this DPA, including the Validation & Security Pack on the [Trust Center](#) and written answers to reasonable questionnaires. If that is not enough, or an authority requires it, the Customer may audit CMCfy, once a year unless there has been a breach, on 30 days' notice, during business hours, under confidentiality, and at the Customer's cost. Audits of CMCfy's providers are carried out through their own certifications and reports.

4. The Customer's obligations

The Customer is responsible for having a lawful basis for the personal data it provides, for the instructions it gives, and for the content its users choose to send with CMCfy Writer. The Customer will not send special category data or directly identifying data about patients or study subjects with CMCfy Writer, and will pseudonymise or remove such data first. The Customer may switch CMCfy Writer off, or connect it to its own cloud account instead (Enterprise), in which case that provider acts under the Customer's own contract and is not CMCfy's subprocessor.

5. Subprocessors

The Customer gives CMCfy general authorisation to use subprocessors. The current list is in Annex III and on the [Privacy Policy](#). CMCfy will give at least 30 days' notice of a new subprocessor by updating that list and the [update log](#), and by email to Customers who ask for notices at sales@cmcfy.com. The Customer may object on reasonable data protection grounds within that period; the parties will try to agree a solution, and if they cannot, the Customer may end the affected part of the Agreement and receive a pro-rata refund of prepaid fees for it. CMCfy imposes data protection terms on each subprocessor that are no less protective than this DPA and remains responsible for its subprocessors.

6. International transfers

CMCfy and its subprocessors are in the United States. Where Customer personal data is transferred from the European Economic Area to CMCfy, the parties enter into the Standard Contractual Clauses adopted by the European Commission in Decision (EU) 2021/914 (the "Clauses"), which are incorporated into this DPA by reference: Module Two (controller to processor) where the Customer is a controller, and Module Three (processor to processor) where it is a processor. For the Clauses: clause 7 (docking) applies; under clause 9(a), option 2 (general written authorisation) applies with the 30-day notice in section 5; the optional wording in clause 11 does not apply; under clause 13, the supervisory authority is the one competent for the Customer; the Clauses are governed by Irish law (clause 17) and disputes go to the courts of Ireland (clause 18). Annexes I to III of this DPA complete the Clauses' Annexes.

United Kingdom. For transfers from the UK, the International Data Transfer Addendum to the EU Clauses issued by the UK Information Commissioner (version B1.0) applies, with Table 1 to 3 completed by this DPA and either party able to end it as allowed by Table 4. **Switzerland.** For transfers from Switzerland, the Clauses apply with references to the GDPR read as the Swiss Federal Act on Data Protection, the Swiss FDPIC as the competent authority, and Swiss data subjects able to bring claims in Switzerland.

If an authority or court asks CMCfy for Customer personal data, CMCfy will challenge requests that are unlawful, disclose the minimum required, and tell the Customer unless the law forbids it.

7. Liability and term

Each party's liability under this DPA is subject to the limits in the Agreement, except where Data Protection Law or the Clauses do not allow a limit. This DPA lasts as long as CMCfy processes Customer personal data under the Agreement.

Annex I. Details of the processing

Data exporter	The Customer, as named in the Agreement or the signature block. Activity: using CMCfy for its regulatory, quality and development work. Role: controller (or processor).
Data importer	Accolade Software Products LLC, c/o Harvard Business Services, Inc., 16192 Coastal Hwy, Lewes, DE 19958, United States. Contact: sales@cmcfy.com. Activity: providing CMCfy. Role: processor (or subprocessor).
Data subjects	The Customer's users of CMCfy and its staff who contact CMCfy; and any people the Customer's users choose to mention in text sent with CMCfy Writer.
Categories of data	Users: name, work email, company, job title, plan, sign-in records, access codes (scrambled), usage counts, support correspondence. Writing text: whatever the user approves in the "What will be sent" box; the Customer agrees to keep personal data out of it as far as possible.
Special category data	None intended. The Customer agrees not to send it (section 4).
Frequency	Continuous for accounts; one-off for each writing request, only when a user presses a CMCfy Writer button.
Nature and purpose	Hosting, sign-in, applying plan limits, support, and passing approved text to the writing service and the result back to the user.
Retention	Writing text: not stored by CMCfy; held only in memory while the request runs. Usage counters: about 40 days. Account data: for the Agreement, then deleted within 90 days. Support email: up to 3 years after last contact.
Subprocessors	As in Annex III, for the same subject matter, nature and duration.

Annex II. Technical and organisational measures

- **Data minimisation by design:** the tools process files in the browser; a Content Security Policy on every tool page blocks connections to anywhere except the writing service; users see and approve the exact text before it is sent.
- **No storage of content:** writing and chat text pass through memory only and are not logged; errors are logged by status code alone.
- **Encryption:** HTTPS (TLS 1.2 or later) for all traffic, with HSTS; providers encrypt stored data.
- **Access control:** administrator accounts (hosting, code, email, domain, payments) use two-factor sign-in and are limited to the people who need them; provider keys are held as encrypted secrets, never in code or in the browser.
- **Software integrity:** code is reviewed before release; each release is versioned and fingerprinted, and the IQ/OQ in the validation pack lets the Customer verify it.
- **Abuse protection:** rate limits, the Cloudflare network's attack protection, and a person check on the public chat.
- **Resilience:** the service runs on Cloudflare's global network; the tools also work from an offline copy, so the Customer's work does not depend on our servers.

- **Providers:** chosen for recognised security certifications (for example SOC 2 or ISO 27001) and bound by data protection terms.
- **Incidents:** a documented process to assess, contain and notify breaches within the time in section 3.

Annex III. Subprocessors

Provider	Where	What it does for CMCfy	What it sees
Cloudflare, Inc.	United States (global network)	Hosts cmcfy.com and app.cmcfy.com, protects them from attacks, runs the "are you a person?" check (Turnstile) and keeps the monthly usage counters	Network address, browser details and the pages requested; usage counters keyed by a scrambled (hashed) code
Anthropic, PBC	United States	Writes the text for CMCfy Writer and answers questions in the Ask CMCfy chat on the website	Only the text a user approves and sends (CMCfy Writer) or types (chat). Not used to train models
Microsoft Corporation (Microsoft 365)	United States	Our email (sales@cmcfy.com and support@cmcfy.com)	The emails you send us and our replies
Google LLC (Google Analytics)	United States	Counts visits to the website, only after a visitor presses Accept on the cookie notice	Pages visited, approximate location, device and browser, a random cookie ID
Clerk, Inc. (when accounts launch)	United States	Sign-in and user accounts	Name, work email, company, sign-in records
Stripe, Inc. (when online payments launch)	United States	Payments, invoices and subscriptions	Name, billing email and address, company, tax ID, payment card details (held by Stripe; we never see the full card number)

Signatures

Signed by the authorised representatives of the parties.

Customer (data exporter)	Accolade Software Products LLC (data importer)
Signature	Signature
Name	Name
Title	TitleManaging Member
Date	Date

Customer legal name, address and contact for data protection notices:
