

Data Processing Agreement

Last Updated: September 8, 2026

This Data Processing Agreement ("DPA") forms part of the Terms of Service between Agely LLC ("Agely", the "Processor") and the community owner or organization that uses Agely to verify its members (the "Customer", the "Controller"). It applies wherever the Customer is subject to the EU General Data Protection Regulation (GDPR), the UK GDPR, or the Swiss Federal Act on Data Protection, and it is written to meet Article 28 GDPR.

It is accepted by using the Service. A Customer who needs a signed copy can download this agreement as a PDF, complete the signature block at the end, and send it to privacy@agely.xyz; Agely will countersign and return it.

1. Definitions

"Personal Data", "Processing", "Controller", "Processor", "Sub-processor", "Data Subject", "Personal Data Breach", and "Supervisory Authority" have the meanings given in the GDPR. "Member" means a Data Subject who verifies with Agely at the Customer's request. "Service" means Agely's age verification service as described in the Terms of Service.

2. Roles of the Parties

The Customer is the Controller of Member Personal Data processed through the Service, and Agely is its Processor. Agely acts as an independent Controller only for the Customer's own dashboard account, support and deletion requests sent to Agely directly, its own billing and usage records, and its website analytics. This DPA does not cover that independent processing, which is described in Agely's Privacy Policy.

3. Details of the Processing

This section serves as Annex I to the Standard Contractual Clauses referred to in Section 10.

- Subject matter: verification of Members' age for access to the Customer's community
- Duration: the term of the Customer's use of the Service, plus the retention periods in Section 8
- Nature and purpose: collecting a date of birth, selfie, video, or government ID image from a Member; estimating age and extracting a date of birth using automated analysis; matching a face to an ID and running an optional liveness check; delivering the outcome to the Customer; and, where the Customer has enabled it, attaching the redacted proof image to the delivered result
- Categories of Data Subjects: the Customer's community members and applicants, and the Customer's moderators who action a result
- Categories of Personal Data: platform user ID (a Discord user ID, or an opaque identifier for web and app tenants); date of birth (processed transiently); computed age and age band; verification method, outcome, timestamps, and rejection reason; the estimated age range, face-match score, and liveness outcome recorded with the result; the identifier of the message the result was delivered in; and the ID of a moderator who approves, rejects, or resets a result
- Special categories: facial images and video (biometric data) and government ID images, processed transiently for age estimation, liveness, and identity matching only
- Optional feature: where the Customer enables birthday announcements and a Member opts in, that Member's birth date is stored for that community only, until the Member removes it or the Customer removes Agely
- Frequency: continuous, each time a Member starts a verification
- Parties (Annex I.A): the Customer named in the signature block, as data exporter and controller, and Agely LLC, as data importer and processor, contactable at the address and email given on this page. The activities relevant to the transfer are those described above
- Competent supervisory authority (Annex I.C): as identified in Section 10

- Pseudonymous records kept by Agely: a hashed record of each Member's written release (text version, locale, time) kept for five years as evidence of consent, and a hashed twelve-month block for a Member rejected at a computed age under 13. Both are keyed by a one-way salted hash of the platform user ID and are not reversible into a list of Members

4. Customer Instructions

Agely processes Member Personal Data only on the Customer's documented instructions, which consist of the Terms of Service, this DPA, the verification workflows and settings the Customer configures in the dashboard, and the commands and actions the Customer's moderators take in the Service. Instructions outside those channels are accepted only where Agely agrees to them in writing, and Agely may charge for work needed to carry them out. Agely informs the Customer if it believes an instruction infringes data protection law, and may suspend processing of that instruction until the point is resolved without being in breach of this DPA. Agely may process Personal Data otherwise only where required by law, in which case it informs the Customer before processing unless the law prohibits it.

5. Customer Obligations

The Customer is responsible for the following:

- Establishing and documenting a lawful basis for requiring verification and for the processing of biometric and ID data, including any written release required by state biometric laws where the Customer has enabled proof media being shared with its moderators, verifiable parental consent for Members under 13 in the United States, and parental consent for Members below the local age of digital consent in the EU/EEA and the UK
- Informing Members about the verification, for example in the community's rules or privacy notice, including that Agely is used as a processor
- Configuring the Service appropriately, including whether proof media is attached to results and who can see the result channel
- Handling Member proof it receives (for example, an image in its moderation channel) in line with its own obligations, and deleting it when no longer needed
- Responding to Data Subject requests it receives, using the tools Agely provides

6. Confidentiality

Agely ensures that persons authorized to process Personal Data are bound by confidentiality obligations. Access is limited to what is needed to operate and support the Service.

7. Security Measures

Agely implements the following technical and organizational measures (Article 32 GDPR). This section serves as Annex II to the Standard Contractual Clauses.

- Encryption in transit (TLS) and at rest for all stored data
- Verification media held only in access-restricted private storage, never on public URLs, and deleted automatically once the result is delivered (seconds in the normal case; 24 hours at most)
- AI analysis by Amazon Web Services with AI-service data retention opted out, so images are analyzed transiently and not retained by the provider
- No storage of dates of birth or biometric templates; only the outcome, computed age, age band, and method are retained
- Role-based access controls and authenticated administrative access; production access limited to Agely personnel who need it
- Destructive deletion (permanent removal, not flagging) for all deletion paths
- Logging and monitoring of the Service for errors and abuse, with rate limiting on verification attempts

8. Retention and Deletion

- Verification media: deleted within seconds of the result being delivered; 24 hours at most
- Date of birth: used to compute age, then discarded
- Unfinished sessions: expire after 24 hours and are swept
- Undelivered results (no result channel configured): held for at most 24 hours, then discarded
- Member outcome (status, computed age, age band, method, timestamps): retained until the Member deletes it, the Member leaves the community (which clears the age band and reason and redacts the delivered card, keeping only the bare verdict), or the Customer's configured re-verification interval expires
- When the Customer removes Agely: birthdays saved for that community are deleted immediately. Member outcomes are retained so a returning community does not need to re-verify, and any Member can delete theirs at any time. On written request, Agely uses commercially reasonable efforts to delete all remaining Member Personal Data for the Customer's community within 30 days
- At the end of the Service, the Customer chooses whether Agely deletes the remaining Member Personal Data or returns it, and Agely acts on that choice within 30 days of a written request. Where the Customer asks for return, Agely provides the outcome records as a structured export; there is nothing further to return, because Agely holds no media and no dates of birth beyond what this section describes. If the Customer makes no choice within 30 days of the end of the Service, Agely deletes. Agely may retain Personal Data where a law it is subject to requires it, and where it does, it keeps only what that law requires, keeps it confidential, and deletes it when the requirement ends. Backups are overwritten on their ordinary cycle
- Written-release records: Agely keeps a hashed record of each Member's biometric release for five years as evidence of consent, as an independent controller under its legitimate interest in demonstrating compliance with biometric privacy laws. These records are not deleted on the Customer's instruction and are swept automatically at five years
- Under-13 blocks: a Member rejected at a computed age under 13 has their identified records removed at once and a hashed block kept for twelve months, cleared earlier by the Member's own /reset, on a parent's request, or by the Customer's deletion request

9. Sub-processors

The Customer gives general authorization for the Sub-processors listed below, all established in the United States. Agely engages each of them under a written data protection agreement no less protective than this DPA and remains liable to the Customer for their performance, subject to Section 14, with one exception: where the Customer's community is a Discord server, Discord operates that platform under its own terms with the Customer and its members, Agely cannot instruct it, and Agely is not liable for Discord's own processing. Agely publishes changes to this list on its Data & Security page at least 14 days before a new Sub-processor processes Member Personal Data, and informs the Customer in writing within the same period, by email to the Customer's dashboard account where one exists and otherwise in the community's configured log channel. A Customer may object on reasonable data protection grounds within that period, in which case the parties discuss the objection in good faith. If no resolution is found, the Customer's sole and exclusive remedy is to stop using the Service. Replacing a Sub-processor in an emergency, to keep the Service running or to address a security issue, may take effect immediately, with notice as soon as practicable afterwards. This section serves as Annex III to the Standard Contractual Clauses.

- Amazon Web Services, Inc.: biometric age estimation, ID text extraction, face matching, and liveness checks
- Vercel Inc.: hosting, transient private media storage, and cookieless website analytics
- Neon, Inc.: database (outcomes and settings only)
- Discord Inc.: the platform the Customer's community runs on and where results are delivered. Discord processes that data under its own terms with the Customer and its members, not on Agely's instructions
- Clerk, Inc.: dashboard sign-in for the Customer's account

10. International Transfers

Agely is established in the United States and processes Personal Data there. For transfers from the EU/EEA, the Customer and Agely enter into the European Commission's Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), Module Two (controller to processor), which are incorporated into this DPA by reference with the Customer as data exporter and Agely as data importer. The following choices apply: the optional docking clause in Clause 7 is included; in Clause 9(a), Option 2 (general written authorisation) applies, with 14 days' notice of any change of Sub-processor; the optional wording in Clause 11(a) about an independent dispute resolution body is not included; under Clause 17, Option 1 applies and the Clauses are governed by the law of Ireland; under Clause 18(b), disputes are resolved before the courts of Ireland, which does not affect a Member's right under Clause 18(c) to bring proceedings in the courts of the country where they live. Annex I.A is completed by the parties named in this DPA and its signature block; Annex I.B by Section 3; Annex I.C by the supervisory authority of the EU member state in which the Customer is established, or, where the Customer is not established in the EU/EEA, the supervisory authority of the member state in which the Members concerned are located. Section 7 is Annex II and Section 9 is Annex III. For transfers from the UK, the Information Commissioner's International Data Transfer Addendum (version B1.0) is incorporated, with Table 1 completed by the parties named in this DPA, Tables 2 and 3 by the Clauses and Annexes above, and Table 4 allowing either party to end the Addendum under its Section 19; as that Addendum requires, the Clauses are then governed by the law of England and Wales and disputes are heard by the courts of England and Wales. For transfers from Switzerland, the Clauses apply with the adaptations required by the Swiss Federal Data Protection and Information Commissioner: the Commissioner is the competent authority, references to the GDPR are read as references to the Swiss Federal Act on Data Protection, and Members in Switzerland may bring proceedings in Switzerland. Agely's Sub-processors are bound by equivalent transfer clauses.

11. Assistance to the Customer

Taking into account the nature of the processing, Agely assists the Customer with responding to Data Subject requests (Members can delete their own data at any time with /reset; other requests sent to Agely are forwarded to the Customer within 5 business days, or handled directly where the Customer instructs it), with the security of processing, with Personal Data Breach notification, and with data protection impact assessments and prior consultation, by providing the information in this DPA and on the Data & Security page.

12. Personal Data Breach

Agely notifies the Customer without undue delay after becoming aware of a Personal Data Breach affecting Member Personal Data, and will use commercially reasonable efforts to do so within 48 hours. The notification describes, to the extent then known, the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed. Where the full information is not available at once, Agely provides it in phases as it becomes available. Notification goes to the email on the Customer's dashboard account, and where no dashboard account exists, to the community owner through the platform the community runs on. Notification is not an admission of fault or liability by Agely.

13. Audit and Information

Agely makes available the information necessary to demonstrate compliance with Article 28 GDPR: this DPA, the Data & Security page, and written answers to reasonable questions sent to privacy@agely.xyz. Where that is insufficient to satisfy a legal requirement, the Customer may, at most once a year and on 30 days' written notice, conduct or mandate an audit of Agely's processing, limited to the Service and carried out in a way that does not disrupt it or expose other customers' data. Agely may charge its reasonable costs for audits beyond the written information above.

14. Liability, Term, and Precedence

Each party's liability under this DPA is subject to the limitations and exclusions in the Terms of Service, including the aggregate cap in Section 14 of those Terms, and claims under this DPA and under the Terms of Service count together toward that single cap. Neither party is liable to the other under this DPA for indirect, incidental, special, consequential, or punitive damages, or for loss of profits, revenue, or goodwill. Nothing in this section limits a Data Subject's rights against either party under Article 82 GDPR, or either party's liability to a Supervisory Authority, and where one party

pays compensation or a fine for which the other is responsible under Article 82, it may recover that share from the other party subject to the cap above. Nothing in this section excludes liability that cannot be excluded by law. This DPA takes effect when the Customer first uses the Service and continues until Agely has deleted or returned all Member Personal Data for the Customer under Section 8. Where this DPA conflicts with the Terms of Service, this DPA prevails for the processing it covers; where it conflicts with the Standard Contractual Clauses, the Clauses prevail.

Signature (optional)

This DPA applies by using the Service. If your organization requires a signed copy, download the PDF, complete the Customer details, sign, and email it to privacy@agely.xyz. Agely will countersign and return it, normally within 5 business days.

Customer (Controller)	Agely LLC (Processor)
Legal name	Legal name
	Agely LLC
Community (for example, Discord server name and ID)	Address
	7901 4th St N, Ste 300, St. Petersburg, FL 33702, United States
Address	Name and title of signatory
	James Eades, Authorized Member
Name and title of signatory	Signature
Signature	Date
Date	

Agely LLC

A Florida limited liability company, Document No. L24000426977

7901 4th St N, Ste 300, St. Petersburg, FL 33702, United States

Represented by James Eades, Authorized Member

Email: privacy@agely.xyz

Discord Support Server: <https://discord.gg/mFGC2yHkr8>