



Data Processing Agreement

ALUMA FZ-LLC (trading as aluma)

For customers of aluma, including UK and UAE processing

Document control

Document reference	ALU-DPA-001
Version	1.1
Date created	6 October 2026
Issue date	13 October 2026
Next review date	October 2027, or sooner if the law or the Services change
Policy owner	Data Protection Lead
Approved by	Kate Markham, Founder
Classification	Public: may be shared with customers and prospective customers

Version history

Version	Date	Summary of changes
0.1	October 2026	General UK and UAE template prepared by CyberWhite.
1.0	6 October 2026	Tailored to aluma: details completed from the privacy policy and Terms; breach notice aligned to 48 hours; storage location corrected to the UK; deletion, export and audit log terms added; measures matched to aluma's security policy.
1.1	13 October 2026	Schedule 1 updated: monthly wellbeing check-ins (staff ratings from 1 to 5 stars, chat requests and check-in dates) added to the personal data processed, and their automatic deletion after 2 years added to retention.

DATA PROCESSING AGREEMENT

This Data Processing Agreement (the “DPA”) forms part of the aluma Terms of Service published at aluma.app/terms (the “Agreement”) between:

- the business that holds an aluma account and has accepted the Agreement (“Customer”); and
- ALUMA FZ-LLC (trading as “aluma”), a free zone company incorporated in the United Arab Emirates with registration number 47037088, whose registered office is at CWEP8123, Compass Building, Al Shohada Road, Al Hamra Industrial Zone-FZ, Ras Al Khaimah, United Arab Emirates (“Provider”).

Customer and Provider are each a “Party” and together the “Parties”.

Background

- Customer determines the purposes and means of processing the Personal Data described in Schedule 1 and is the Controller, or acts on behalf of a Controller, for that Personal Data.
- Provider processes that Personal Data for Customer to provide aluma, an online service that helps children’s activity businesses and nurseries manage staff records, compliance, venues and governance (the “Services”). Customer Data is stored in the United Kingdom. Provider is established in the United Arab Emirates (“UAE”), and its personnel access Customer Data remotely from the UAE to provide and support the Services.
- The Parties intend this DPA to satisfy applicable data-protection requirements governing the processing, security and international transfer of Personal Data, including, where applicable, the UK GDPR, the Data Protection Act 2018, the EU GDPR and the UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Personal Data (“UAE PDPL”), together with applicable implementing regulations and sector or free-zone requirements.
- This DPA applies to the processing of Personal Data under the Agreement. The Agreement and this DPA are collectively the “Contract”. This DPA takes effect when Customer accepts the Agreement, and no signature is needed. A signed copy is available on request (Schedule 6).

1. Definitions and interpretation

1.1 Definitions

“Applicable Data Protection Law” means all laws and regulatory requirements applicable to the processing of Personal Data under the Contract, including, where applicable: (a) the UK GDPR and the Data Protection Act 2018; (b) the EU GDPR; (c) the UAE PDPL and applicable implementing regulations; (d) applicable DIFC, ADGM or other UAE free-zone data-protection law where relevant to a Party or processing activity; and (e) applicable sector-specific privacy, confidentiality, cybersecurity, employment, health or regulatory requirements.

“Controller”, “Data Subject”, “Personal Data”, “Personal Data Breach”, “Process”/“Processing”, “Processor”, “Supervisory Authority” and “Special Category Data” have the meanings given in the Applicable Data Protection Law. Where UAE law applies, these terms include the equivalent concepts under the UAE PDPL.

“Customer Data” means all Personal Data and other information submitted to, collected by or generated through the Services on Customer’s behalf.

“International Transfer” means a transfer, disclosure, remote access or other making available of Personal Data from one jurisdiction to another where the transfer is restricted by Applicable Data Protection Law.

“Restricted Transfer” means a transfer restricted under the UK GDPR or EU GDPR, including a transfer of Personal Data from the UK or EEA to the UAE where no adequacy decision or other lawful transfer mechanism applies.

“Sub-processor” means any Processor appointed by Provider to process Personal Data on Customer’s behalf.

“Transfer Impact Assessment” or “TIA” means a documented assessment of the legal, practical and technical circumstances of an International Transfer, including the laws and practices of the destination country and the effectiveness of supplementary measures.

- 1.2** Order of precedence. If there is a conflict between this DPA and the Agreement, this DPA prevails in relation to the processing and protection of Personal Data, unless the Agreement gives the Personal Data more protection. If there is a conflict between this DPA and an applicable statutory transfer mechanism, the statutory transfer mechanism prevails to the extent required by law. Nothing in the Contract limits a Data Subject’s or Supervisory Authority’s statutory rights.

2. Roles and documented instructions

- 2.1** Customer is the Controller and Provider is the Processor in respect of the Personal Data processed by Provider for the Services, except where Schedule 1 expressly identifies a different relationship.
- 2.2** Provider shall process Personal Data only on Customer’s documented instructions, including the Agreement, this DPA, Schedule 1 and subsequent written instructions. Provider shall not:
- sell, rent or disclose Personal Data for its own purposes;
 - use Personal Data for advertising or profiling, or to train artificial intelligence models;
 - combine Personal Data with data from another customer, except where Customer has chosen to share it (for example with a linked Head Office account); or
 - determine the purposes or means of processing except to the limited extent necessary to provide the Services and comply with law.
- 2.3** Customer’s instructions include processing necessary to provide, secure, support, maintain and improve the Services only as described in Schedule 1. Provider shall promptly notify Customer if, in its reasonable opinion, an instruction infringes Applicable Data Protection Law. Provider shall not be required to follow the instruction until Customer confirms or changes it, unless Applicable Data Protection Law requires the processing.
- 2.4** Customer’s instructions also include the choices Customer makes when using the Services, such as inviting staff to the staff portal, sharing records through an inspection link or with a linked Head Office account, setting retention periods, exporting data, and deleting records or its account.
- 2.5** Customer is responsible for ensuring that its instructions, collection and use of Personal Data have a lawful basis and comply with Applicable Data Protection Law, including the

extra conditions for health data, criminal-offence data and data about children. Provider shall provide reasonable assistance to enable Customer to meet those responsibilities.

3. Compliance with UAE requirements

- 3.1 Provider shall comply with the UAE PDPL and other Applicable Data Protection Law applicable to Provider or its processing in the UAE.
- 3.2 Provider shall maintain records and documentation required by Applicable Data Protection Law, including records describing Customer, Provider, authorised personnel, categories of Personal Data, processing purposes and periods, erasure arrangements, cross-border movements and technical and organisational measures, and shall make them available to Customer or the competent UAE authority where legally required.
- 3.3 Provider has appointed a Data Protection Lead as its data-protection contact (Schedule 5) and shall notify Customer of changes. Provider has assessed that a Data Protection Officer is not currently required, keeps this under review, and shall appoint one if Applicable Data Protection Law requires it.
- 3.4 Provider shall not process Personal Data after the authorised processing period or outside the agreed scope unless Customer authorises an extension or Applicable Data Protection Law requires continued retention. Provider shall securely return or erase Personal Data at the end of the Services, as set out in Section 13.

4. Confidentiality and authorised personnel

- 4.1 Provider shall keep Personal Data confidential and shall ensure that personnel authorised to process it:
 - access only the Personal Data necessary for their role, and only to run and support the Services;
 - are bound by written confidentiality obligations or a statutory duty of confidentiality;
 - receive appropriate privacy and security training; and
 - process Personal Data only on documented instructions.
- 4.2 Provider shall maintain an up-to-date list of categories of personnel with access to Personal Data and shall provide it to Customer on reasonable request, subject to security and confidentiality restrictions.

5. Technical and organisational measures

- 5.1 Provider shall implement and maintain appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access and other unlawful processing. The measures are set out in Schedule 2.
- 5.2 Provider shall apply privacy and security by design and by default, including data minimisation, least privilege, separation of each customer's data and secure configuration.
- 5.3 Provider shall not materially reduce the security of the Services during the term. Provider shall notify Customer before making a material change that is reasonably likely to reduce the security or privacy protections described in Schedule 2.
- 5.4 Provider shall maintain a written security incident-response plan and business-continuity and disaster-recovery arrangements appropriate to the Services. Provider shall test those arrangements at least once a year and address identified weaknesses.

6. Personal Data Breaches

- 6.1** Provider shall notify Customer without undue delay and, in any event, within 48 hours after becoming aware of a Personal Data Breach affecting Customer Data. The notification shall include, to the extent known:
- the nature and timing of the breach;
 - the categories and approximate number of Data Subjects and records affected;
 - likely consequences;
 - containment and corrective measures taken or proposed;
 - the relevant incident reference and contact; and
 - any information reasonably required for Customer's regulatory, contractual or Data Subject notifications.
- 6.2** Where not all of this information is known at first, Provider shall give it in stages as it becomes available. Provider shall promptly investigate, contain, remediate and document the breach, preserve relevant evidence and provide regular updates. Provider shall not notify a Supervisory Authority or Data Subject about a breach involving Customer Data without Customer's prior written approval, unless legally required; if legally required, Provider shall notify Customer before doing so where lawful.
- 6.3** Provider shall cooperate with Customer in meeting notification deadlines and responding to Supervisory Authorities, Data Subjects and other affected parties. Provider shall not make admissions about Customer's responsibility without Customer's approval.

7. Data Subject rights and assistance

- 7.1** Taking into account the nature of the processing, Provider shall assist Customer by appropriate technical and organisational measures to respond to requests to exercise Data Subject rights, including access, rectification, erasure, restriction, objection and portability, where applicable.
- 7.2** Provider shall:
- notify Customer promptly, and within 48 hours where practicable, if it receives a Data Subject request relating to Customer Data;
 - not respond to the request except on Customer's documented instructions or where required by law;
 - provide the relevant Personal Data in a commonly used and machine-readable format where required (Customer can also export its data at any time from the Services); and
 - correct, delete or restrict processing as instructed by Customer, subject to legal retention requirements.

8. Assistance with compliance and assessments

- 8.1** Provider shall provide reasonable assistance with Customer's data-protection impact assessments, legitimate-interest assessments, security assessments, consultations with Supervisory Authorities and records of processing.
- 8.2** Provider shall promptly provide information reasonably necessary to demonstrate compliance with this DPA, including current security documentation, certifications (if any), policies, penetration-test summaries and Sub-processor information, subject to reasonable confidentiality and security restrictions.

- 8.3** Provider shall inform Customer of any law, regulatory order or official request that prevents or materially limits Provider from complying with Customer's instructions, unless prohibited by law. Provider shall assess the request, limit disclosure to the minimum legally required, challenge it where there are reasonable grounds to do so and document its response.

9. Sub-processors

- 9.1** Customer gives Provider general written authorisation to appoint the Sub-processors listed in Schedule 3. Provider shall:
- give at least 30 days' prior notice of any proposed addition or replacement, by email to Customer's account owner and by updating its published list of providers;
 - provide information reasonably necessary for Customer to assess the Sub-processor;
 - impose written obligations providing at least the same level of protection as this DPA;
 - remain fully responsible for the acts and omissions of each Sub-processor; and
 - ensure that each Sub-processor complies with the International Transfer provisions in Section 10.
- 9.2** Customer may object on reasonable data-protection grounds within the notice period. The Parties shall work in good faith to resolve the objection. If no reasonable solution is available, Customer may terminate the affected Service on written notice without penalty, and Provider shall refund the unused part of any period Customer has paid for.
- 9.3** If a Sub-processor must be replaced urgently to protect Customer Data or keep the Services running, Provider may make the change on shorter notice. Provider shall tell Customer as soon as possible, and Customer keeps its right to object under Section 9.2.
- 9.4** Provider shall not appoint a Sub-processor in a jurisdiction that would create an additional Restricted Transfer without putting in place the required transfer mechanism and supplementary measures before the transfer begins.

10. International transfers and UAE processing

- 10.1** Customer Data is stored in the United Kingdom (London). Customer authorises: (a) Provider's personnel in the UAE to access Customer Data remotely, solely to provide and support the Services; and (b) the Sub-processor transfers listed in Schedules 3 and 4.
- 10.2** Provider shall not transfer, access or permit access to Customer Data from another country unless the transfer is listed in Schedule 3 or 4, or Customer has approved it, and the transfer complies with Applicable Data Protection Law.
- 10.3** The Parties shall rely on the following transfer mechanisms, in this order of preference:
- an applicable adequacy decision or equivalent approved protection level;
 - the UK International Data Transfer Agreement (IDTA), or the UK International Data Transfer Addendum to the EU Standard Contractual Clauses, where the UK GDPR applies;
 - the EU Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 (Module 2 for controller-to-processor transfers, Module 3 for processor-to-processor transfers), where the EU GDPR applies;
 - another lawful mechanism recognised by the relevant Applicable Data Protection Law; or
 - a derogation or exception, only where the legal conditions are met and documented.

- 10.4** For Restricted Transfers from Customer to Provider under the UK GDPR, the current ICO-approved IDTA is incorporated into this DPA, with its Part 1 tables completed using Schedules 1 to 5. The Parties shall not amend its mandatory clauses except as the approved form permits.
- 10.5** Where the EU GDPR applies, the applicable EU SCC module is incorporated into this DPA in its current official form, completed using Schedules 1 to 4. Module 3 applies if Customer is itself a processor; otherwise Module 2 applies.
- 10.6** Provider shall complete a TIA for its transfers to the UAE and to Sub-processors in the United States, review it whenever there is a material change in the destination country, law, service, Sub-processor, data, transfer route or risk, and give Customer a summary on request.
- 10.7** Supplementary measures include:
- encryption in transit and at rest using strong industry-standard cryptography;
 - strict role-based access, with two-factor sign-in for Provider's administrator access;
 - separation of each customer's data at database level;
 - no use of Customer Data for Provider's own purposes or to train artificial intelligence models;
 - logging of access to sensitive records;
 - secure deletion on the timetable in Section 13;
 - transparency about, and challenge of, disproportionate government requests; and
 - the technical and organisational measures in Schedule 2.
- 10.8** Provider shall notify Customer promptly if it cannot comply with the applicable transfer mechanism, if it receives a legally binding request for access to Customer Data, or if it reasonably believes the transfer mechanism is no longer effective. Provider shall suspend the affected transfer if instructed by Customer or required by law, and shall cooperate on an alternative lawful arrangement.
- 10.9** Provider shall not make an onward transfer unless it is authorised, subject to the required transfer mechanism and disclosed in Schedule 3 or 4, or approved under Section 9.
- 10.10** If a competent authority requires the Parties to use a new or replacement transfer mechanism, the Parties shall cooperate to implement it. If compliance is not possible, Customer may suspend the affected transfer or terminate the affected Service without prejudice to its other rights.

11. Government and law-enforcement access

- 11.1** If Provider receives a request from a public authority for Customer Data, Provider shall, unless prohibited by law:
- notify Customer before disclosure;
 - refer the authority to Customer where legally and practically possible;
 - assess whether the request is lawful and binding;
 - disclose only the minimum data legally required;
 - seek a protective order or other remedy where reasonably available; and
 - keep a record of the request and response.

- 11.2** Provider shall not voluntarily disclose Customer Data to a public authority except as legally required, as expressly authorised by Customer, or where needed to protect someone from serious harm.

12. Audits and inspections

- 12.1** Provider shall make available information necessary to demonstrate compliance with this DPA and shall allow audits by Customer or an independent auditor appointed by Customer, no more than once a year unless a Personal Data Breach, material non-compliance or a regulator requirement justifies more frequent review.
- 12.2** Provider may first answer an audit request with documents, such as this DPA, Provider's security policies, a completed security questionnaire and its latest penetration-test summary. A further audit may take place where those are not enough, on at least 30 days' notice, during normal business hours, and in a way that avoids unnecessary disruption or disclosure of another customer's information. Customer shall bear its own audit costs, except that Provider shall bear the reasonable costs of an audit required because of Provider's material breach.
- 12.3** Provider shall promptly address material audit findings and provide a remediation plan with target dates. Nothing limits a Supervisory Authority's audit or inspection powers.

13. Retention, return and deletion

- 13.1** Provider shall retain Customer Data only for the period and purposes in Schedule 1 or as otherwise instructed by Customer. Provider shall not retain Personal Data indefinitely merely because storage is available. Customer can set retention periods for the main types of record in the Services.
- 13.2** Return. Customer can export all Customer Data at any time from the Services (records as spreadsheet files and uploaded documents in one download), including while its account is paused or cancelled, until the data is deleted. Provider shall help with an export on request.
- 13.3** Deletion. When Customer's account closes, for any reason, Customer instructs Provider to delete Customer Data on this timetable: live data 30 days after closure; backup copies of uploaded files within a further 30 days; database backups within 7 days after the live data is deleted. If a free trial ends without a subscription, the same timetable runs from the end of the trial. Provider shall confirm deletion in writing on request.
- 13.4** Audit log. Provider keeps a log of who viewed or changed sensitive records (not the contents of those records) for 6 years after the account closes, as a Controller, to deal with legal claims and support safeguarding investigations, as described in Provider's privacy policy. Where other law requires retention, Provider shall protect the retained data and process it only for that purpose.
- 13.5** Provider shall ensure that its Sub-processors delete or return Customer Data on the same basis and shall obtain confirmation where reasonably requested.

14. Obligations after termination

Sections 4, 5, 6, 8, 10, 11, 13, 14, 15 and any provisions intended by their nature to survive shall continue after termination for as long as Provider retains or can access Customer Data.

15. Liability

The Parties' liability for data-protection breaches is governed by the liability provisions in the Agreement, subject always to any mandatory rights or liabilities under Applicable Data Protection Law.

16. Term and termination

- 16.1** This DPA begins when the Agreement begins and continues while Provider processes Customer Data.
- 16.2** Customer may require Provider to suspend processing or terminate the affected Services if Provider materially breaches this DPA, cannot comply with an applicable transfer mechanism, or creates a material risk that cannot reasonably be remediated.

17. Notices and contacts

- 17.1** Data-protection notices shall be sent to the contacts in Schedule 5, and may also be sent under the notice provisions in the Agreement.
- 17.2** Each Party shall promptly notify the other of changes to its legal name, establishment, data-protection contact, Supervisory Authority, processing locations or material transfer arrangements.

18. General

- 18.1** This DPA takes effect on acceptance of the Agreement. Where a signed copy is made, it may be signed electronically and in counterparts.
- 18.2** If any provision is invalid, the remaining provisions remain effective and the Parties shall replace the invalid provision with a valid provision that most closely achieves its purpose.
- 18.3** Neither Party may assign this DPA except as permitted by the Agreement and only if the assignee is bound by equivalent data-protection obligations.
- 18.4** Provider may update this DPA to reflect changes in law or in the Services, giving Customer at least 30 days' notice of any change that reduces the protection of Customer Data. The current version is published at aluma.app.
- 18.5** This DPA is governed by the law of England and Wales, as the Agreement is, subject to any mandatory governing-law, forum or third-party-beneficiary provisions in the IDTA, UK Addendum or EU SCCs.

Schedule 1: Processing details

Customer / Controller	The business named in the aluma account. Contact: the account owner, at the email address held in the account.
Provider / Processor	ALUMA FZ-LLC (trading as aluma), Ras Al Khaimah, United Arab Emirates. Contact: Data Protection Lead, hello@aluma.app.
Services	aluma, an online service for children's activity businesses and nurseries to manage staff records, checks and documents, venues, policies, payroll paperwork, the accident and incident book, safeguarding records and inspection readiness, with a staff portal for the business's own staff.
Subject matter	Hosting and processing the records Customer chooses to keep in the Services.
Duration	The term of the Agreement, plus the deletion periods in Section 13.
Nature of processing	Collection through the app and staff portal, storage, organisation, display, reminders and notifications, sharing when Customer chooses (for example an inspection link or a linked Head Office account), backup, export and deletion.
Purposes	Providing, securing and supporting the Services for Customer.
Data Subjects	Customer's staff members (employed, self-employed and volunteers) and applicants; their referees and emergency contacts; venue contacts; children and the parents or carers recorded in the accident and incident book; adults hurt at a session, such as staff or visitors; people who make a complaint to a nursery; and Customer's own users of the Services.
Personal Data	Staff details (name, role, contact details, date of birth, home address, emergency contact, contract, dates, pay and payroll details, sessions worked, invoices, pay changes, employment status checks, messages); checks and documents (certificates and qualifications, right to work documents, references, suitability declarations, signed contracts, appraisals, supervision notes, onboarding checks, policy sign-offs); monthly wellbeing check-ins (a 1 to 5 star rating, whether the staff member asked for a chat, and when their manager checked in); accident and incident book entries; nursery complaints (complainant's name and contact details); user account and sign-in details; and the audit log of access to sensitive records.
Special category data	Health data in the accident and incident book (injury, treatment, body map). Safeguards: access limited by role, every view logged, never included in inspection links or partner packs.
Criminal-offence data	DBS certificate details and copies, Update Service details, overseas criminal record checks, suitability declarations, and referrals to the Disclosure and Barring Service or Local Authority Designated Officer (LADO). Safeguards: access limited by role, views logged, a staff member's own DBS copy stays private to them.

Children's data	Only in the accident and incident book: the child's name, age or date of birth, room, what happened, injury, treatment, body map, and which parent or carer was told (their name and how they were contacted). No photographs of people are held, except a right to work identity document.
Frequency	Continuous, while Customer uses the Services.
Processing location	Stored in the United Kingdom (London). Accessed remotely by Provider's personnel in the UAE. Sub-processors as listed in Schedule 3.
Retention	Customer sets retention periods for the main record types; the Services flag records past their date for Customer to review. Monthly wellbeing check-ins are deleted automatically after 2 years. All Customer Data is deleted on the timetable in Section 13.
Customer instructions	The Agreement, this DPA, and Customer's settings and use of the Services.
Automated decision-making	None. The Services show reminders and status colours; they do not make decisions about individuals.
Regulatory requirements	Customer remains responsible for its own sector duties, such as Ofsted and the EYFS, safeguarding guidance, DBS rules and RIDDOR reporting.

Schedule 2: Technical and organisational measures

Provider maintains the following measures, appropriate to the risks of the processing. They are described in general terms; more detail is available to Customer on request, subject to confidentiality.

1. Governance and accountability

- Written Information Security, Access Control, Data Retention and Data Breach Response policies, and a data protection impact assessment, each reviewed at least once a year.
- A named Data Protection Lead responsible for information security and for checking providers.
- Registered with the UK Information Commissioner's Office.
- Confidentiality obligations for everyone with access to Customer Data.
- Certifications: none held at present. Provider is working towards Cyber Essentials and will update this Schedule when it is achieved.

2. Access control

- Each customer's data is separated at database level, and an automated test proves on every change that one customer cannot reach another's data.
- Role-based access: Customer decides what its staff can see through the staff portal.
- Strong passwords and email verification; optional two-factor sign-in for users; lockout after repeated failed sign-ins; bot protection on public forms.
- Provider's administrator access uses a separate named account with two-factor sign-in.
- Provider's personnel access Customer Data only to run and support the Services, never for routine browsing.

3. Encryption

- Encryption in transit everywhere, with strict secure-connection settings.
- Encryption at rest for the database, uploaded files and backups.
- Keys and credentials held securely outside the code, with automated checks that none are committed.

4. Application and infrastructure security

- Every change is reviewed and passes automated checks (code quality, tests, customer-separation test, security scanning, secret scanning and dependency checks), then is tested on a staging copy before going live.
- Automatic alerts and a weekly sweep for vulnerable software components, and a monthly security audit.
- Uploaded files are checked by type and size, and only served to signed-in users of the right business through short-lived links.
- Private links (such as inspection links) carry a secret code, expire, can be withdrawn and are logged when viewed.
- Industry-leading hosting and security technologies, with standard browser security protections on the website and app.

5. Data management

- Data minimisation: no data about children or parents except in the accident and incident book and nursery complaints; no photographs of people except a right to work identity document.
- An append-only audit log of every view or download of sensitive records, which no one, including Provider, can edit or delete.
- Customer-set retention periods, export at any time, and deletion on the timetable in Section 13.
- Daily database backups and nightly encrypted backups of uploaded files, held in the UK and Europe. A full restore has been tested and is repeated at least once a year.
- Error reports have private links, web address details and anything typed into forms removed before they are sent.

6. Physical and environmental security

- Customer Data is hosted with established cloud providers that maintain physical, environmental and power protection of their data centres. Provider runs no data centre of its own.
- Provider's devices are kept secure: firewall on, updates applied, and strong unique passwords held in a password manager.

7. International transfers and government access

- Approved processing locations and transfer routes are documented in Schedules 1, 3 and 4.
- Transfer impact assessments, onward-transfer controls and the government-request procedure in Section 11.

8. Testing and assurance

- An independent penetration test of internet-facing systems at least once a year (the first is scheduled for October 2026), with a summary available to Customer on request.
- Documented remediation of material findings.
- Annual review of this Schedule.

Schedule 3: Approved Sub-processors

These providers process Customer Data for Provider. Providers that Provider uses as a Controller for its own purposes (such as payments, its own emails to account owners and website statistics) are listed in its privacy policy at aluma.app/privacy. Changes are made under Section 9.

Sub-processor	Service and processing	Location	Transfer safeguard
Supabase	Database, sign-in and file storage	Stored in the United Kingdom (London); Supabase staff and its sub-processors in the United States and Singapore may access it to run and support the service	EU SCCs (Module 2) with UK terms, under Supabase's DPA and transfer impact assessment
Vercel	App hosting	Servers in London; US company	Provider's DPA with Vercel; UK safeguard under Schedule 4
Cloudflare (R2)	Encrypted backup copies of uploaded files	Europe	Not needed (UK adequacy for the EU)
Cloudflare (Turnstile)	Bot checks on sign-in and public forms (IP address and browser details)	United States	Provider's DPA with Cloudflare; UK safeguard under Schedule 4
Resend	Sending service emails and reminders	Sends from its European region (Ireland); Resend is a US company and its main processing is in the United States	UK Addendum to the EU SCCs, and the UK Extension to the Data Privacy Framework, under Resend's DPA
Sentry	Error reports, with form contents and private links removed	Stored in its EU region (Germany); Sentry is a US company and may also process in the United States	UK Addendum to the EU SCCs, and the UK Extension to the Data Privacy Framework, under Sentry's DPA
Anthropic	Reading term dates from a document Customer chooses to upload; not used to train models	United States	Provider's DPA with Anthropic; UK safeguard under Schedule 4

Sub-processor	Service and processing	Location	Transfer safeguard
Browser push services (Google, Apple, Mozilla)	Delivering notifications if a user turns them on; content is encrypted	Mainly United States	Content encrypted end to end; UK safeguard under Schedule 4

Schedule 4: International transfers

Exporting location (law)	Importing location	Data	Purpose	Transfer mechanism	Supplementary measures
United Kingdom (UK GDPR)	UAE (Provider)	All Customer Data in Schedule 1, by remote access	Running and supporting the Services	UK IDTA, incorporated under Section 10.4	Section 10.7 and Schedule 2
United Kingdom (UK GDPR)	United States (Sub-processors in Schedule 3)	As listed in Schedule 3	As listed in Schedule 3	UK Addendum to the EU SCCs, or the UK Extension to the EU-US Data Privacy Framework, under each provider's DPA	Encryption in transit and at rest; minimum data sent
UAE (UAE PDPL)	United Kingdom (storage)	All Customer Data of UAE customers	Storing and running the Services	Contractual safeguards in this DPA, and any further controls required under the UAE PDPL	Section 10.7 and Schedule 2
EEA (EU GDPR)	UAE / United Kingdom	Only if Customer is subject to the EU GDPR	As above	EU SCCs Module 2 (or Module 3), under Section 10.5	Section 10.7 and Schedule 2

Transfer impact assessments: Provider keeps a TIA for its transfers to the UAE and the United States under Section 10.6, and gives Customer a summary on request.

UAE requirements: the Parties document the legal basis for transfers under the UAE PDPL. Where the UAE PDPL's requirements for transfers to a destination without an approved protection level apply, the Parties use the contractual safeguards in this DPA and any other controls required by the UAE PDPL, its implementing regulations or competent authority guidance. Provider keeps records of cross-border movements and cooperates with Customer in documenting the transfer.

Schedule 5: Contacts

Role	Customer	Provider
Contract contact	Account owner (email held in the account)	hello@aluma.app
Data-protection contact	Account owner, or the contact Customer names	Data Protection Lead, hello@aluma.app
Data Protection Officer	If Customer has one	Not currently required (Section 3.3)
Security incident contact	Account owner	Data Protection Lead, hello@aluma.app (breach notices are sent any day, within 48 hours)
Sub-processor notices	Account owner's email	Sent by Provider; list published at aluma.app/privacy
Supervisory Authority	Customer's own regulator	UK Information Commissioner's Office (registration ZC252716)
UAE regulator	If applicable	UAE Data Office, where applicable

Schedule 6: Signature (optional)

This DPA takes effect when Customer accepts the Agreement, without a signature. If Customer would like a signed copy, both Parties may sign below.

Signed for and on behalf of the Customer (business name): _____

Name: _____

Title: _____

Signature: _____

Date: _____

Signed for and on behalf of ALUMA FZ-LLC

Name: _____

Title: _____

Signature: _____

Date: _____