

BudgetUp data processing agreement (template)

UK GDPR Article 28 controller-to-processor agreement for institutions

Template: subject to review by your legal team. This is BudgetUp's standard starting draft. It is not legal advice, and it has not yet been reviewed by our own solicitor. We will also sign your institution's own DPA, or Jisc or consortium model clauses, where you prefer.

Version 0.1 (template) · Prepared 8 October 2026 · Owner: Tamsar Global Ltd (data protection lead)

Parties

1. **The Customer** (the "**Controller**"): the institution named in the order form or licence agreement, such as a university, further education college, council, housing association or employer.
2. **Tamsar Global Ltd** (the "**Processor**"), trading as BudgetUp, a company registered in England and Wales under company number 17371733, registered office Unit 3, Office A, 1st Floor, 6-7 St Mary At Hill, London EC3R 8EE. Contact: privacy@budgetup.uk.

Background

A. The Controller has licensed BudgetUp, a gamified financial education service, under a licence agreement, pilot agreement or order form (the "**Main Agreement**").

B. In providing BudgetUp to the Controller's learners, the Processor processes personal data on the Controller's behalf. This agreement sets out the terms required by Article 28(3) of the UK GDPR and section 59 of the Data Protection Act 2018.

C. Where a person signs up to BudgetUp directly (the free plan or Plus) and not through the Controller, Tamsar Global Ltd is the controller for that person's data, and this agreement does not apply to it.

1. Definitions

1.1 "**Data Protection Legislation**" means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) and any other law that applies to the processing, as amended or replaced from time to time.

1.2 "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Special Categories of Personal Data**" and "**Supervisory Authority**" have the meanings given in the UK GDPR. The Supervisory Authority is the Information Commissioner's Office (ICO).

1.3 "**Sub-processor**" means any third party the Processor engages to process Personal Data on the Controller's behalf.

1.4 "**Restricted Transfer**" means a transfer of Personal Data outside the United Kingdom that is not covered by UK adequacy regulations.

1.5 "**IDTA**" means the International Data Transfer Agreement issued by the ICO under section 119A of the Data Protection Act 2018, and "**UK Addendum**" means the ICO's International Data Transfer Addendum to the European Commission's Standard Contractual Clauses.

2. Roles and scope

2.1 The Controller determines the purposes and means of processing learners' Personal Data. The Processor processes it only to provide BudgetUp under the Main Agreement.

2.2 Schedule 1 describes the subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of Data Subjects.

2.3 Where the Processor uses pseudonymised or aggregated data for research or service improvement, it does so only as described in Schedule 1, paragraph 8, and only where the Data Subject has given separate research consent.

3. The Processor's obligations

3.1 **Documented instructions.** The Processor processes Personal Data only on the Controller's documented instructions, including on transfers outside the UK, unless UK law requires otherwise. If so, the Processor tells the Controller before processing, unless the law prohibits this. This agreement, the Main Agreement and the Controller's configuration of BudgetUp (for example, switching the AI coach on or off, enabling single sign-on or setting under-18 mode) are the Controller's instructions. The Processor tells the Controller immediately if it believes an instruction breaks the Data Protection Legislation.

3.2 **Confidentiality.** The Processor ensures that everyone authorised to process the Personal Data is bound by a duty of confidentiality, contractual or statutory.

3.3 **Security.** The Processor implements the technical and organisational measures in Schedule 2, as required by Article 32 of the UK GDPR. It may update them, provided the overall level of protection does not fall.

3.4 Sub-processors. The Processor complies with clause 4.

3.5 Data Subject rights. Taking into account the nature of the processing, the Processor helps the Controller, by appropriate technical and organisational measures, to respond to requests to exercise Data Subjects' rights. In particular:

(a) learners can download their data (JSON or readable HTML), correct their details and delete their account themselves in the app, under Settings, "Your data and account";

(b) the Processor passes any request it receives from a learner enrolled by the Controller to the Controller without undue delay and does not respond to it except on the Controller's instructions, unless the learner is exercising a self-service right in the app; and

(c) the Processor provides any other help the Controller reasonably needs within **10 working days** of the Controller's request.

3.6 Help with compliance. Taking into account the nature of the processing and the information available to it, the Processor helps the Controller meet its obligations under Articles 32 to 36 of the UK GDPR, including security, breach notification, data protection impact assessments and prior consultation with the ICO. The Processor provides a pre-filled DPIA summary on request.

3.7 Personal Data Breaches. The Processor notifies the Controller **without undue delay, and in any event within 24 hours**, of becoming aware of a Personal Data Breach affecting the Controller's Personal Data. The notification includes, as far as then known: the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. The Processor provides further information as it becomes available, takes reasonable steps to contain and mitigate the breach, and does not notify Data Subjects or the ICO about the Controller's data without the Controller's agreement unless the law requires it.

3.8 Deletion or return. On termination or expiry of the Main Agreement, the Processor deletes or, at the Controller's choice, returns all Personal Data processed for the Controller **within 30 days**, and deletes existing copies, unless UK law requires storage. Encrypted backups are overwritten on their normal cycle and are gone **within 35 days** of deletion from the live database. Records the Processor must keep for its own legal obligations (for example invoices) are kept as its own controller records and are listed in the privacy notice.

3.9 Audit and information. The Processor makes available all information necessary to show compliance with Article 28 and allows for and contributes to audits, including inspections, by the Controller or an auditor it mandates. The parties agree that, in the first instance, this is met by the Processor answering a written security and privacy questionnaire once a year (or after a Personal Data Breach), and by providing its security overview, sub-processor register and any

certifications it then holds. An on-site or remote audit beyond this may be carried out once a year, on 30 days' written notice, during business hours, under confidentiality terms, at the Controller's cost unless it reveals a material breach of this agreement.

3.10 Records. The Processor keeps a record of processing activities carried out on behalf of the Controller, as required by Article 30(2) of the UK GDPR.

4. Sub-processors

4.1 The Controller gives general written authorisation for the Processor to use the Sub-processors listed in Schedule 3.

4.2 The Processor gives the Controller at least **30 days' notice** before adding or replacing a Sub-processor that will process the Controller's Personal Data, by email to the Controller's nominated contact and by updating the register at <https://budgetup.uk/trust>. The Controller may object on reasonable data protection grounds within that period. The parties then discuss the objection in good faith. If they cannot resolve it, the Controller may end the affected part of the Main Agreement without penalty and receive a pro rata refund of prepaid fees for it.

4.3 The Processor imposes on each Sub-processor, by written contract, data protection obligations that give at least the same protection as this agreement, in particular sufficient guarantees of appropriate technical and organisational measures.

4.4 The Processor remains fully liable to the Controller for each Sub-processor's performance of its obligations.

5. International transfers

5.1 The Processor's primary hosting and database are in the European Union (Germany). The UK has adequacy regulations for the EU and EEA, so these transfers are not Restricted Transfers.

5.2 The Processor does not make a Restricted Transfer of the Controller's Personal Data unless one of the following applies, and Schedule 3 shows which: (a) the destination is covered by UK adequacy regulations, including the UK Extension to the EU-US Data Privacy Framework for a certified US recipient; or (b) the Processor, or its Sub-processor, has entered into the **IDTA** or the **UK Addendum** with the recipient, with a transfer risk assessment carried out and supplementary measures applied where needed.

5.3 On request, the Processor provides a copy of the relevant transfer mechanism (with commercial terms removed) and a summary of its transfer risk assessment.

6. The Controller's obligations

6.1 The Controller is responsible for: having a lawful basis for the processing, and for any Special Categories of Personal Data; giving learners a privacy notice that covers BudgetUp (the Processor's notice at <https://budgetup.uk/legal/privacy> can be linked); the accuracy of data it provides (for example through single sign-on, SCIM or rostering); and the instructions it gives.

6.2 Where the Controller enrolls learners aged 16 or 17, it sets its tenant to under-18 mode (or lets the age question decide) and carries out its own DPIA, which the Processor will help with.

6.3 The Controller decides whether to switch on optional features, including the AI coach for adult learners, and is responsible for that decision.

7. Liability, term and precedence

7.1 Each party's liability under this agreement is subject to the limits and exclusions in the Main Agreement, except where the law does not allow liability to be limited. **[Legal: agree the cap, and whether data protection liability sits inside or outside it.]**

7.2 This agreement lasts as long as the Processor processes Personal Data for the Controller, and clauses 3.8 and 3.9 survive termination.

7.3 If this agreement conflicts with the Main Agreement on data protection, this agreement wins. If the parties sign model clauses offered by the Controller (for example Jisc or consortium clauses), those clauses win where they conflict with this template.

7.4 This agreement is governed by the law of England and Wales, and the courts of England and Wales have exclusive jurisdiction.

Signatures

	Controller	Processor: Tamsar Global Ltd
Name		
Role		Director
Signature		
Date		

Schedule 1: Processing details

1. Subject matter. Providing BudgetUp, a gamified UK financial education service (lessons, games, arcade, review cards, money plan, optional AI coach for adults, institution reporting), to learners the Controller enrolls, and to the Controller's staff who administer it.

2. Duration. The term of the Main Agreement, plus the deletion period in clause 3.8.

3. Nature of processing. Collection (through sign-up, single sign-on, LTI, SCIM or access codes), storage, organisation, retrieval, use to deliver learning and track progress, aggregation into suppressed institution reports, transmission to the Controller's systems where the Controller configures it (LTI grade passback, xAPI, SCORM or cmi5), and erasure.

4. Purposes. (a) Delivering learning and saving progress; (b) letting learners sign in through the Controller's identity provider; (c) institution reporting on engagement and outcomes, as suppressed aggregates; (d) optional pre- and post-programme check-in surveys; (e) the optional AI coach for adult learners, where the Controller switches it on; (f) support, safety and security of the service.

5. Categories of Data Subjects.

- Learners the Controller enrolls: students, apprentices, further education learners (including those aged **16 and 17**), residents and tenants, and employees.
- The Controller's staff who administer BudgetUp (institution administrators and analysts).

6. Categories of Personal Data.

Category	Examples	Notes
Identity and contact	Name, display name, email address, a generated pseudonym	Email is optional for some sign-in routes (for example access codes)
Institution identifiers	SSO subject ids (SAML pairwise-id, Entra tid and oid, Google sub), LTI user ids, SCIM directory ids, cohort and group membership	Supplied by the Controller's systems
Age band	16–17, 18–20, 21–24, 25–34, 35+ or "prefer not to say"	Only the band is stored, never a date of birth. It switches on under-18 mode
Learning activity	Levels played, scores, stars, XP, streaks, badges, review schedule, game saves, in-game behaviour signals, money plan answers	
Onboarding and check-in answers	Goals, situation, interests; optional confidence and wellbeing check-ins	Check-ins are optional
Optional equality information	Lower-income household, first in family, disabled or a long-term health condition, mature, care-experienced, estranged, ethnicity, and similar access and participation characteristics	Optional , collected only with explicit consent. Disability and ethnicity are Special Categories of Personal Data. Encrypted separately and never shown individually to staff

Category	Examples	Notes
AI coach conversations	Question text, answers, safety classifications, cited lesson ids	Adults only, only when the Controller switches the coach on and the learner accepts the first-use notice. Kept 90 days
Support and feedback	Problem reports and feedback the learner sends	
Technical and security	Session records, hashed rate-limit counters, audit log entries (account id only)	

7. Special Categories. Only the optional equality information above, processed only with the learner's explicit consent (Article 9(2)(a)). Learners may also volunteer health or other sensitive information in free text to the AI coach; the safeguards are in Schedule 2. No criminal offence data is intentionally processed.

8. Research and aggregates. Institution reports are computed live and suppress any group under 10 learners. Pseudonymised research use takes place only with the learner's separate research consent.

9. Retention. As in the BudgetUp retention schedule (<https://budgetup.uk/legal/privacy>), including: AI coach conversations 90 days; inactive accounts deleted after 24 months; data held for the Controller deleted or returned within 30 days of contract end; backups overwritten within 35 days; security and audit logs up to 6 years, holding an account id only.

Schedule 2: Technical and organisational measures

This schedule describes the measures in place on 8 October 2026. Items marked **(planned)** are not yet in place; we list them so you can see the gap.

Access and tenant isolation

- PostgreSQL row-level security (RLS) separates each institution's data. The application connects as a role that cannot bypass RLS; a separate authentication role can reach only the four sign-in tables; the owner role is used only for migrations, content sync and backups.
- Automated RLS tests run against a real database as the restricted app role on every change in continuous integration, covering cross-tenant reads, staff scopes, the audit log, billing, the AI coach and integration APIs.
- Institution staff see only suppressed aggregates (groups under 10 hidden) and cannot read AI coach conversations or equality information.
- Platform operator access is limited to named accounts and audit-logged.

Encryption

- In transit: HTTPS everywhere through Cloudflare (TLS 1.2 or higher at the edge), HTTP Strict Transport Security, and an encrypted Cloudflare Tunnel from the edge to the origin, so the origin server exposes no public web port.
- Optional equality information: encrypted at the application layer with AES-256-GCM, with a dedicated key held outside the database.
- Backups: encrypted on the server (rclone crypt) before they leave it.
- Database volume: full-disk encryption (LUKS) is part of our dedicated database server build. **(planned)** It is not yet in place on the interim shared production host.

Data minimisation and privacy by design

- Only an age band is stored, not a date of birth. No names or email addresses are sent to the AI model.
- Under-18 mode (ICO Children's Code): no AI coach, no analytics, no browser error reports, no marketing prompts, no individual leaderboards, no social features, no nudges, weekly not daily streaks.
- Analytics (PostHog EU) runs only with the learner's consent and never in under-18 mode. Event properties are limited to slugs, numbers and booleans; identity is a one-way hash; session recordings mask all text and never run on settings, admin, coach or parent pages.
- No advertising pixels run inside the learning app. Advertising tags exist only on public marketing pages, only with separate marketing consent, and never in under-18 mode.

AI coach safeguards (where the Controller switches it on)

- Off by default for every institution; always off for under-18s; a first-use notice; rate limits and a daily spend cap per learner.
- Deterministic safety rules route crisis, self-harm, scam-in-progress, debt emergency and under-18 messages to fixed replies with helplines, without generating an AI answer.
- Answers are grounded only in reviewed BudgetUp lessons, checked sentence by sentence before display for product names, recommendations and wrong key figures.
- Conversations are kept 90 days, visible only to the learner, and never used to train models.

Resilience and backups

- Nightly logical database backup, kept 7 days on the server and 30 days off-site in Cloudflare R2 (EU jurisdiction), encrypted before upload.
- Automated monitoring: an external uptime check every 5 minutes, and a server watchdog that alerts on unhealthy services, low disk or memory, and missing or stale backups.

Logging and accountability

- An append-only audit log (the application role cannot update or delete it) records security and data-rights events, such as exports, deletions, role changes and coach settings. It holds account ids, never names or email addresses.
- A data-subject request queue with statutory deadlines, plus self-service export and deletion for learners.

People and process

- Staff and contractors are bound by confidentiality. Access to production is restricted to named individuals.
- Personal data breach procedure: assess, contain, notify the Controller within 24 hours, then review.
- Secure development: typecheck, automated tests and RLS tests on every change; secrets kept out of source control.
- **(planned)** Cyber Essentials certification for Tamsar Global Ltd (the parent company, Tamsar Inc, holds Cyber Essentials, but it does not yet cover this company), an independent penetration test before public launch, and HECVAT 4.

The full detail is in the BudgetUp security overview, available on request or at <https://budgetup.uk/trust>.

Schedule 3: Sub-processors

Generated from the live register (`apps/web/src/components/marketing/subprocessors.ts`), which is also published at <https://budgetup.uk/trust>. "At launch" means the provider goes live with our public launch; "planned" means it starts when the feature it supports launches. Providers marked as **independent controllers** (Google LLC and LinkedIn for advertising measurement, Google Ireland for Sign in with Google) are listed for transparency. They are not Sub-processors of the Controller's data: advertising tags never run inside the learning app, and Sign in with Google is the learner's own choice.

Sub-processor	Purpose	Location	Transfer mechanism	Status
Hetzner Online GmbH	Hosting, database, object storage, backups	Germany (Nuremberg, Falkenstein)	UK adequacy (EU)	In use
Cloudflare, Inc.	Secure tunnel, DNS, CDN, web application firewall and DDoS protection; encrypted off-site database backups in R2 (EU jurisdiction)	Global edge; backups stored in the EU	IDTA / UK Addendum; Data Privacy Framework	In use
Google LLC (Gemini API, paid tier)	Ask Nana, the optional AI money coach for adults (Gemini models). Processes questions only to generate answers; paid-tier terms, so no training on customer data; names, emails and card or phone numbers are masked before sending. Switched off for under-18s and per institution. Before any institution enables the coach we move it to Google Cloud Vertex AI in London (europe-west2)	United States / global	UK Extension to the EU-US Data Privacy Framework; IDTA / UK Addendum	In use (adults, optional)
Stripe Payments Europe Ltd	Plus subscriptions (hosted checkout, card details never reach us), refunds and institution licence invoices. Only for people who buy Plus and for institutions we invoice	Ireland / United States	UK adequacy (EU); IDTA / UK Addendum	At launch
Google Ireland Ltd (Sign in with Google)	Optional "Continue with Google" sign-in: confirms your name and verified email. Google is an independent controller for your Google account; we receive no tokens we keep and send nothing about your learning	Ireland / United States	UK adequacy (EU); Data Privacy Framework	In use (optional)
Brevo (Sendinblue SAS)	Transactional email (sign-in links, receipts)	France	UK adequacy (EU)	In use
Functional Software, Inc. (Sentry), EU region	Error monitoring. Server errors always; browser errors only with analytics consent and never in under-18 mode. Names, emails, IP addresses, cookies, request bodies and codes in links are removed before sending	Germany (Frankfurt, de.sentry.io)	UK adequacy (EU); IDTA / UK Addendum for US support access	Optional (not currently used; errors go to PostHog EU)

Sub-processor	Purpose	Location	Transfer mechanism	Status
PostHog Inc, EU Cloud	Product analytics: pages viewed, masked button taps, lesson and game events, page speed, and masked session recordings for about 1 in 4 visits (all text and typing hidden; never on settings, admin, coach or parent pages). Only with analytics consent and never in under-18 mode. No cookies, no IP addresses stored; identity is a one-way hash of the account id. Reached through our own /ingest address	Germany (Frankfurt, eu.posthog.-com)	UK adequacy (EU); IDTA / UK Addendum for US support access	In use (consent only)
Google LLC (Google Analytics 4, Google Ads)	Measuring our advertising on our public website pages only (never in the learning app), with Google Consent Mode v2 and only after marketing consent; never in under-18 mode. Google signals and enhanced conversions off; no names or emails sent. Google is an independent controller for its ad measurement	United States / global	UK Extension to the EU-US Data Privacy Framework; IDTA / UK Addendum	When ads run (marketing consent only)
LinkedIn Ireland Unlimited Company (Insight Tag)	Measuring our LinkedIn adverts on our public website pages only (never in the learning app), only after marketing consent and never in under-18 mode. No names or emails sent. LinkedIn is an independent controller for its ad measurement	Ireland / United States	UK adequacy (EU); UK Extension to the EU-US Data Privacy Framework (LinkedIn Corporation)	When ads run (marketing consent only)

Transfers outside the UK and EU (UK IDTA / UK Addendum). Where a Sub-processor above may process data in the United States or elsewhere outside the UK and EU, the transfer relies on, in order: the UK Extension to the EU-US Data Privacy Framework where the recipient is certified; otherwise the IDTA or the UK Addendum to the EU Standard Contractual Clauses in that provider's data processing terms. This applies to Cloudflare (global edge network), Stripe (US group processing), and US support access for Sentry and PostHog. The AI coach's production processing is planned for Google Cloud Vertex AI in London (europe-west2), a domestic UK transfer. **Current position (8 October 2026):** the coach currently runs on the Google Gemini API, and the move to Vertex AI europe-west2 is pending. We will not switch the coach on for any institution's learners until that move is complete, and we will update this schedule when it is.