

BudgetUp security questionnaire answers

Pre-filled answers to common higher education vendor questions (HECVAT-lite style)

Version 0.1 · 8 October 2026 · Tamsar Global Ltd (trading as BudgetUp), company 17371733 ·
Contact: privacy@budgetup.uk

These are short, honest answers to the questions UK universities and colleges ask most often. They are not a completed HECVAT 4; that is **planned**. Where the answer is "no" or "planned", we say so. Detail is in the BudgetUp security overview and DPA template.

Company and assurance

#	Question	Answer
1	Legal entity and registration	Tamsar Global Ltd, England and Wales, company 17371733. Registered office: Unit 3, Office A, 1st Floor, 6-7 St Mary At Hill, London EC3R 8EE. Wholly owned by Tamsar, Inc. (Delaware, USA)
2	ICO registration	Yes. Tamsar Global Ltd is registered with the ICO, registration number ZC269951
3	Cyber Essentials / Cyber Essentials Plus	Our parent company, Tamsar, Inc., holds Cyber Essentials (IASME, valid to July 2027). Certification in Tamsar Global Ltd's own name, and Cyber Essentials Plus, are planned
4	ISO/IEC 27001, SOC 2	Yes, Tamsar Global Ltd is certified to ISO/IEC 27001; the certificate is available on request. SOC 2 only if we sell in the US
5	Independent penetration test	Not yet. A CREST-accredited test is planned before public launch, then yearly
6	Completed HECVAT	Not yet. HECVAT 4 is planned; these answers are the interim version
7	Cyber insurance / professional indemnity	Quotes to be obtained; bound on contract award (we'll confirm cover levels in the bid)
8	Named security contact	The company director, via hello@budgetup.uk (subject "Security report")

Data and hosting

#	Question	Answer
9	Where is data hosted?	Hetzner Online GmbH, Germany (EU). Off-site backups: Cloudflare R2, EU jurisdiction
10	Is data transferred outside the UK/EU?	Core data, no. Some sub-processors may process limited data in the US (Cloudflare edge, Stripe for payments, US support access for Sentry and PostHog) under the UK Extension to the EU-US Data Privacy Framework or the IDTA / UK Addendum. See DPA Schedule 3
11	Can you offer UK-only hosting?	Not today. The deployment is portable and can move to a UK host if required by contract
12	What personal data do you process?	Name, email (optional on some routes), SSO identifiers, age band (not date of birth), learning activity, optional surveys, optional equality information (explicit consent), optional AI coach chats (adults only). See DPA Schedule 1

#	Question	Answer
13	Do you process special category data?	Only optional equality information (disability or health condition, ethnicity), with explicit consent, encrypted separately, never shown individually to staff
14	Data processing agreement?	Yes: our Article 28 template, or your own / Jisc model clauses
15	Sub-processor list and change notice	Published at budgetup.uk/trust ; 30 days' notice with a right to object
16	Retention and deletion at contract end	Deleted or returned within 30 days; backups overwritten within 35 days. Full schedule in the privacy notice
17	Do you sell data, show ads or use data for advertising?	No. No ads in the product, no ad pixels in the learning app, no data sales
18	Is customer data used to train AI models?	No
19	Support for data subject requests	Self-service export, correction and deletion in the app; operator queue with statutory deadlines; help to the institution within 10 working days
20	Children (under 18)	Supported for FE learners aged 16 and 17 under an ICO Children's Code mode: no AI, no analytics, no marketing, no social features, no profiling

Security controls

#	Question	Answer
21	Tenant isolation	PostgreSQL row-level security; the app role can't bypass it; automated RLS tests on every change
22	Encryption in transit	Yes. TLS 1.2+ at the Cloudflare edge, HSTS with preload, encrypted tunnel to the origin
23	Encryption at rest	Partly. Special-category fields AES-256-GCM (application layer); backups encrypted before upload. Full-disk encryption of the database server is planned with the move to a dedicated server
24	Backups	Nightly, encrypted, off-site in R2 (EU), kept 30 days, plus 7 days on the server; alerting if a backup is late
25	Disaster recovery targets	Indicative RPO 24 hours, RTO one working day. Not yet contractual
26	Shared infrastructure	Yes, during the pre-revenue phase: production shares a Hetzner server with another Tamsar product, with separate containers, network, database and secrets. A dedicated server is planned
27	Single sign-on	Yes: SAML 2.0 (Shibboleth, ADFS, OpenAthens, Entra SAML) with UKAMF metadata support; Microsoft Entra ID and Google Workspace (OIDC); single logout
28	User provisioning	SCIM 2.0 (Entra ID, Okta), including deprovisioning. Entra SCIM validator: 24/24 checks passed
29	LMS integration	LTI 1.3 Advantage (tested end to end in Moodle 4.5), SCORM 1.2 / 2004, cmi5, xAPI
30	Password policy / MFA for end users	No passwords are stored. Sign-in is by email link, Google or institution SSO, so MFA follows your identity provider
31	MFA for vendor administrators	Being confirmed and enforced across every admin account as part of Cyber Essentials

#	Question	Answer
32	Staff access to customer data	Limited to the company owner; app operator functions are allow-listed and audit-logged. Institution staff can't read learners' AI chats or equality information
33	Audit logging	Append-only audit log of security and data-rights events (account ids only), kept up to 6 years
34	Vulnerability management	Pinned dependencies, CI tests on every change. Automated dependency and secret scanning, a patch SLA and a pen test are planned
35	Vulnerability disclosure	Yes, via hello@budgetup.uk ("Security report"); safe harbour for good-faith research
36	Incident response and breach notice	Documented procedure; notify the institution without undue delay and within 24 hours
37	Background checks	Not yet a formal policy; DBS checks where safeguarding roles require them
38	Security awareness training	Not yet formalised; planned with Cyber Essentials

AI (Ask Nana coach)

#	Question	Answer
39	Is AI used?	An optional AI money coach for adult learners (Google Gemini). Off by default for every institution, always off for under-18s
40	Where does AI processing happen?	Planned: Google Cloud Vertex AI, London (europe-west2). Currently the Gemini API; we won't switch the coach on for institution learners until the move is complete
41	Safeguards	Deterministic safety routing (crisis, self-harm, scams, debt) before any AI call; answers only from reviewed lessons; every sentence checked for product names, recommendations and wrong figures; red-team suite (73/74 live, 66/66 critical, 8 October 2026)
42	AI data retention	90 days, learner-only access, "Delete my chats" erases immediately

Accessibility

#	Question	Answer
43	Accessibility standard	WCAG 2.2 AA target. Currently partially compliant; see our accessibility statement
44	VPAT / ACR	A self-assessed ACR (VPAT 2.5 style) is available. An independent audit is planned