

Data Protection, Retention and Deletion Policy

Dash Media Limited · Version 1.0 · Effective 27 October 2026 · Review by 27 October 2027 · Owner: Brad Hook, Director, Dash Media Limited

1. Purpose

To define what personal data we collect, why, how it is protected, how long we keep it, and how it is deleted.

2. What we collect and why

PRODUCT	DATA	PURPOSE
FLAME app	Name, work email, organization and team name, assessment responses (25 factors and collaboration style), sign-in and request logs	Producing individual and team reports; account access; security
Values Institute	Email (optional, at results), assessment selections and rankings, an optional country, purchase records for premium guides (handled by the payment provider, Stripe, not stored by us)	Producing the values profile and guides; research and benchmarking in aggregate; account access

We don't collect passwords, payment card numbers, government identifiers, precise location, or health data. Mood and energy ratings in the FLAME assessment are self-reported workplace indicators and are treated as participant data, not as health records.

3. Lawful basis and consent

- FLAME participants take part in a program commissioned by their employer. The employer is the controller of the decision to run the program; Dash Media Limited is the processor of the resulting data. Participants are told on the join screen who can see their results and that sharing is their choice; the privacy notice, linked from sign-in, says what is collected. Taking part is voluntary: nobody is enrolled without opening the link and entering their own email address.
- Values Institute users are told at the point of email capture that their anonymized responses contribute to research and the Global Values Report, with opt-out and account deletion available.
- We enter into a data processing agreement with any client who requests one.

4. Protection

- **In transit:** TLS 1.2 or higher on every connection. HSTS enforced on all domains.
- **At rest:** AES-256 encryption on the Supabase database, file storage, and backups.

- **Access:** Row Level Security policies restrict each participant to their own rows. Administrative access is limited and protected by multi-factor authentication (see Access Control policy).
- **Location:** Participant data is stored and processed in Sydney, Australia. See the Trust Center for the full hosting table.
- **Logs:** Application logs do not contain assessment responses or sign-in codes. Email addresses may appear in authentication logs for troubleshooting; these logs are retained by the provider (Vercel runtime logs for one day, Supabase authentication and database logs for seven days) and are not exported.
- **AI processing:** Where report narratives are generated using the Claude API, only assessment scores and factor labels are sent. Names, email addresses, and organization names are not. The provider does not train on this data and deletes inputs within 30 days.

5. Retention

DATA	RETAINED	THEN
FLAME participant data (active engagement)	For the duration of the client engagement	See next row
FLAME participant data (after engagement)	Until the client asks for deletion	Deleted on request, within 30 days, with written confirmation
Values Institute account data	While the account is active, and until the person asks for deletion	Deleted on request
Aggregated, de-identified statistics	Indefinitely	Contain no names, emails, or team identifiers
Backups	7 days rolling	Overwritten
Email correspondence with clients	7 years (financial records)	Deleted

6. Deletion

- **Client request:** A client may ask for their team's data to be deleted at any time. We action it within 30 days, confirm in writing, and the data leaves backups within the backup retention window.
- **Participant request:** A participant may ask for a copy of their data or its deletion by emailing the security contact. We verify the request against the account email before acting and respond within 30 days.
- **Method:** Deletion removes the rows from the production database. Reports already downloaded by the participant or client are outside our control.
- **Subprocessors:** Deletion from our database removes the data from Supabase. Anthropic retains nothing beyond its 30-day window. Email providers retain message logs per their own policies, listed in the Subprocessors table.

7. Data subject rights

Participants and users may request access, correction, deletion, or a copy of their data in a portable format, and may object to processing. Requests go to the security contact on the Trust Center and are handled within 30 days. There is no charge.

8. Transfers

Data is stored in Australia and processed by subprocessors in Australia and the United States as listed in the Subprocessors table. For clients subject to the GDPR or UK GDPR, our data processing agreement incorporates the relevant standard contractual clauses.

9. Review

Reviewed annually and when a product adds a new category of data.

10. Version history

VERSION	DATE	CHANGE
1.0	2026-10-27	Initial publication