TRILOGY RESEARCH

Annex B · Technical and Organisational Measures

Version 1.0

24 October 2026

CONTACT

Privacy	privacy@trilogyresearch.co.uk
General	hello@trilogyresearch.co.uk
Phone	+44 (0) 345 33 12345

Trilogy Research Limited · Registered in England and Wales No. 14632667 · VAT GB446142800

Annex to the Trilogy Research Limited Data Processing Agreement

These are the measures we apply to personal data we process, for ourselves and for clients. They are proportionate to who we are: a specialist firm run by its directors, with no shared offices and no legacy systems, working through a small set of vetted providers. We review them at each quarterly compliance check and whenever we add a system, and we only ever strengthen them without notice.

1. Who can reach data

- Access to every system is limited to our directors, each under their own login. There are no shared logins and no standing third-party access.
- Every account that holds personal data is protected by two-step sign-in. This is checked before a system is approved and at every quarterly review.
- Passwords and keys are unique, generated, and held only in an encrypted password manager; none is written down, emailed or kept in documents or code.
- Access for any future staff or contractor is granted per system, to the minimum needed, for the duration needed, under a written confidentiality duty, and removed the day it is no longer needed.

2. Devices

- Work is done on company-controlled Apple devices with full-disk encryption, automatic operating-system and security updates, screen lock, and remote wipe available.
- No personal data is held on removable media, personal devices or personal cloud accounts.

3. Data in transit and at rest

- Every connection to our sites, mailboxes, agents and providers is encrypted (TLS). Data at rest with our providers is encrypted by them; our provider assessment checks this before approval.
- Our websites run no advertising or tracking cookies and, where analytics are used, they set no cookies and report only aggregate figures.

4. Providers (sub-processors)

- No provider handles personal data for us until it has passed our supplier approval procedure: written processing terms meeting UK GDPR Article 28, a lawful transfer safeguard for any data leaving the UK with a transfer risk assessment where the law expects one, independent security assurance (SOC 2 Type 2 or equivalent) where available, AI training on our data switched off, and acceptable-use terms that permit our use.
- No provider is paid for, connected or given data before that approval. Each provider's terms are re-read monthly and the provider reviewed quarterly, by scheduled task.
- Our breach-notice contact is set on every provider account, and we require notice of a provider's breach within 48 hours where the provider offers it.

5. Data minimisation and separation

- We collect and keep only the data a service needs. Client data is held in separate workspaces, projects or accounts per client wherever a provider allows, and is never combined across clients.
- Client data is never used for other clients, for our own products or methods, or to train AI models.

Every AI provider we use has training on our data switched off, confirmed in its settings or contract.

– Where a client's system runs on the client's own equipment, no client data is copied off it, including for support or backup.

6. Development and automation

– No personal data is ever placed in source code, configuration files or code repositories. AI tools receive only the personal data a task needs, and only tools approved for that use. Repositories hold logic and documents; data lives only in the approved systems.

– Automated agents act only within the permissions and instructions recorded for them; changes to what they may do are made by pull request and approved by the director before they go live.

– Test and development work uses synthetic or minimal data wherever possible.

7. Resilience and recovery

– Working data lives in providers with their own redundancy and backups; our documents and configuration are version-controlled so any change can be reversed.

– A loss of access to any one provider does not lose data held elsewhere; the systems a client depends on are documented so they can be restored or rebuilt.

8. Logging and monitoring

– Provider audit logs (sign-ins, admin actions) are enabled where offered and reviewed at each quarterly check and after any incident.

– Unusual sign-in alerts from providers go to a monitored mailbox.

9. Personal data breaches

– Any suspected breach is logged at once, assessed within 24 hours for risk to people, and contained. Affected clients are told without undue delay and within 48 hours of our becoming aware. Where we are the controller, the Information Commission (the ICO) is notified within 72 hours where the law requires, and affected people are told where the risk to them is high.

– Every incident, including near misses, is recorded with what happened, what we did and what we changed.

10. Retention and deletion

– Every category of data has a retention period, recorded in our documents and privacy notice, and is deleted or anonymised when it ends. Client data is returned or deleted at the client's choice when a service ends, with backups cleared within 90 days and deletion confirmed in writing on request.

11. People

– One of our directors holds responsibility for data protection and keeps current with ICO guidance. Any future staff or contractor receives data protection training before handling personal data and annually thereafter.

12. Governance

–

A record of processing, legitimate interests assessments, data protection impact assessments where required, a transfer risk assessment, a supplier register and a complaints procedure are kept, version-controlled and dated. Our position was reviewed in depth in October 2026 and is reviewed quarterly.

VERSION 1.0 · LAST UPDATED 24 OCTOBER 2026