Data Processing Agreement & Record of Processing

CyberSafe Coach — "Connect your systems" feature (Microsoft 365 / Google Workspace security check)

CyberSafe Coach Plus Ltd (Company No. 16872486) · Registered office: 124 City Road, London EC1V 2NX · Version 1.0 — 23 June 2026

Part A — Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the agreement between the organisation that enables the Connect feature (the "Controller") and CyberSafe Coach Plus Ltd (the "Processor") for the provision of the CyberSafe Coach platform (the "Services"). It governs the Processor's processing of personal data on the Controller's behalf when the Controller connects its Microsoft 365 or Google Workspace tenant. It is made under and is to be read consistently with the UK GDPR and the Data Protection Act 2018.

1. Roles of the parties

For the Connect feature, the Controller is the connecting organisation, which determines the purposes and means of processing its own directory data. The Processor (CyberSafe Coach Plus Ltd) processes that data only to perform the read-only security-posture check on the Controller's documented instructions. Nothing in this DPA makes the Processor a controller of the connected directory data.

2. Subject-matter, duration, nature and purpose

(a) Subject-matter: a read-only check of the Controller's identity provider (Microsoft 365 / Google Workspace) to produce a security-posture summary.

(b) Duration: for the term the Controller keeps the Connect feature enabled, and until deletion under clause 9.

(c) Nature: automated, read-only retrieval of identity/configuration metadata via OAuth 2.0; computation of a derived summary; storage of that summary only.

(d) Purpose: to show the Controller whether multi-factor authentication is enabled, who holds administrator access, and (optionally) whether there are dormant accounts — to help the Controller improve its security posture.

Full processing details are in Annex 1.

3. Processor obligations (UK GDPR Article 28(3))

The Processor shall:

- (a) process the personal data only on the Controller's documented instructions, including the act of the Controller's administrator initiating and consenting to a connection, unless required to do otherwise by law (in which case it will inform the Controller unless legally prohibited);
- (b) ensure persons authorised to process the data are bound by confidentiality;
- (c) take all measures required by Article 32 — the technical and organisational measures in Annex 2;
- (d) respect the conditions in Article 28(2) and (4) for engaging sub-processors (clause 5);
- (e) taking account of the nature of processing, assist the Controller by appropriate measures in responding to data-subject rights requests;
- (f) assist the Controller in ensuring compliance with Articles 32–36 (security, breach notification, DPIAs, prior consultation), considering the information available to the Processor;
- (g) at the Controller's choice, delete or return the personal data at the end of the provision of services, and delete existing copies unless storage is required by law (clause 9);

- (h) make available all information necessary to demonstrate compliance with Article 28 and allow for and contribute to audits, including inspections, by the Controller or its mandated auditor (clause 8).

The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes data-protection law.

4. Data minimisation and read-only guarantee

The Processor requests only least-privilege, read-only permissions (Annex 1). It cannot change any setting in the Controller's tenant. The access token obtained at connection is used once for the check and then discarded; no refresh token is retained. The Processor stores only a derived summary of the result — not the content of emails, files, or messages, and not the raw directory export.

5. Sub-processors

The Controller gives general authorisation for the Processor to engage the sub-processors listed in Annex 3. The Processor will impose data-protection terms equivalent to this DPA on each sub-processor and remains liable for their performance. The Processor will give the Controller at least 30 days' notice of any intended addition or replacement of a sub-processor, during which the Controller may object on reasonable data-protection grounds.

6. International transfers

Personal data processed under this DPA is hosted within the UK and/or the European Economic Area. The Processor will not transfer personal data outside the UK or EEA without a lawful transfer mechanism under the UK GDPR (e.g. UK adequacy regulations, the International Data Transfer Agreement, or the UK Addendum to the EU SCCs) and appropriate supplementary measures. Where any sub-processor operates outside the UK or EEA, such a mechanism is applied.

7. Personal data breach

The Processor will notify the Controller without undue delay, and in any event within 24 hours, of becoming aware of a personal data breach affecting the Controller's data, and will provide the information the Controller reasonably needs to meet its own obligations under Articles 33–34.

8. Audit

The Processor will make available the security review, sub-processor list and relevant policies on request, and will allow audits no more than once per year (or following a breach) on reasonable notice, subject to confidentiality and minimising disruption.

9. Return and deletion

On termination of the Connect feature or on the Controller's request, the Processor will delete the stored summary and any associated records within 30 days, and confirm deletion in writing, unless retention is required by law. Tokens and raw provider data are not retained (clause 4).

Annex 1 — Details of the processing

Item	Detail
Categories of data subjects	The Controller's personnel who hold accounts in its Microsoft 365 / Google Workspace tenant (staff, administrators, and any other account holders).
Types of personal data	Account identifiers (user principal name / email address, display name, directory object IDs); administrative role assignments (who holds admin rights); multi-factor authentication / authentication-method registration status; (optional, only if the inactive-accounts check is enabled) account enabled/disabled status and last sign-in date.
Special category data	None requested or processed.
Content data	None. No email, file, calendar or message content is accessed.
Permissions requested (read-only)	Microsoft Graph delegated: User.Read.All, UserAuthenticationMethod.Read.All, RoleManagement.Read.Directory, AuditLog.Read.All (required for the authentication-methods registration report used by the core MFA check); plus sign-in (User.Read, openid, email, profile).
Data produced and stored	A derived posture summary only (e.g. counts/flags such as 'MFA enabled: yes/no', number of admins, number of dormant accounts), stored in connector_check_results.
Frequency	On demand, when the Controller's administrator initiates a check.
Retention	Summary retained until the Controller disconnects the feature or for a maximum of 180 days, whichever is sooner, then automatically deleted; deleted within 30 days of a deletion request or disconnection. Access token discarded immediately after use; no refresh token or raw provider data stored.

Annex 2 — Technical and organisational measures (Article 32)

- Least privilege: only read-only, minimal Microsoft Graph scopes are requested. AuditLog.Read.All is included because Microsoft requires it to read the authentication-methods registration report (userRegistrationDetails) used for the core MFA check; in the default check only MFA-registration status and admin role holders are read — no raw sign-in logs or audit logs. Sign-in activity (signInActivity) is read only when the optional inactive-accounts check is enabled.
- Secret handling: the confidential client secret is held server-side only (platform secrets), never in the browser, URL, database or source control.

- Token handling: the access token is used once and discarded; no refresh token is stored; only a derived summary is persisted (data minimisation).
- Access control: results are protected by database Row-Level Security scoped to organisation membership; the OAuth state parameter protects against CSRF.
- Fail-safe gating: a platform-wide master switch AND a per-organisation flag must both be on; requests fail closed if either is off, missing or unreadable. The master switch is platform-owner-only and changes are audit-logged.
- Encryption: data is encrypted in transit (TLS) and at rest by the hosting platform.
- Identity: administrative access to the platform requires multi-factor authentication.
- Assurance: dependency scanning (Dependabot) is enabled; a methodology-led security review (STRIDE / OWASP / OAuth 2.0 BCP) has been conducted with independent four-eyes verification before go-live; the platform is working toward Cyber Essentials Plus and ISO 27001.

Annex 3 — Approved sub-processors

Sub-processor	Purpose / location
Lovable Cloud (Supabase)	Application backend — database, edge functions, secrets storage. Region: UK/EEA (Lovable-managed Supabase).
Vercel	Front-end hosting / CDN. Region: global edge network; does not store the connector result data.

Microsoft / Google are the Controller's own identity providers (the data source), not sub-processors of the Processor.

Part B — Record of Processing entry (Article 30)

Suggested entry for CyberSafe Coach's Record of Processing Activities, covering the Connect feature.

Field	Entry
Processing activity	Read-only security-posture check of a customer organisation's Microsoft 365 / Google Workspace ("Connect your systems" / Connected Check).
Role	Processor (on behalf of the connecting organisation as Controller).
Purpose of processing	Produce a security-posture summary (MFA status, admin access, optional dormant accounts) to help the organisation improve its security.
Categories of data subjects	Account holders in the connecting organisation's tenant.
Categories of personal data	Account identifiers; admin role assignments; MFA/auth-method status; optional account status and last sign-in date. No content data; no special category data.
Recipients	Internal platform only; sub-processors in Annex 3. The summary is shown to the connecting organisation's administrators.
Third-country transfers	Stored data resident in the UK/EEA. Where a sub-processor operates outside the UK/EEA, an appropriate transfer mechanism applies (UK IDTA / UK Addendum to the EU SCCs).
Retention	Derived summary until disconnect or a maximum of 180 days, whichever sooner; tokens/raw data not retained.
Security measures	See Annex 2 (least privilege, server-side secret, one-time token, RLS, fail-safe master switch, encryption, MFA, dependency scanning, independent review).

End of document. Review with a qualified solicitor before issuing to customers.