DATA PROCESSING AGREEMENT

EU Customers Only — GDPR Article 28

Processor	CyberFence Corp
Effective Date	May 12, 2026
Version	1.0
Applicable Regulation	EU GDPR — Regulation (EU) 2016/679
Transfer Mechanism	EU Standard Contractual Clauses (Module 2, June 2021)
Contact	info@cyberfenceplatform.com

This Data Processing Agreement ("DPA") is entered into between CyberFence Corp ("Processor") and the customer subscribing to CyberFence services who is established in the European Economic Area or whose processing activities are subject to the GDPR ("Controller"). This DPA governs the processing of personal data by CyberFence Corp on behalf of the Controller in connection with the CyberFence services (VPN, Breach Monitor, and web application). It forms part of the Terms of Service and, in the event of conflict regarding personal data, this DPA prevails.

1. Subject Matter and Duration

1.1 CyberFence Corp processes personal data solely to provide the Services: (a) VPN — encrypted traffic routing through US-based servers; (b) Breach Monitor — monitoring user-provided email addresses against known breach databases; (c) Account Management — subscription, devices, billing, and support.

1.2 Processing continues for the duration of the active subscription and ceases upon termination, subject to Section 8 (Deletion).

2. Categories of Personal Data and Data Subjects

CyberFence Corp processes the following categories of personal data on behalf of the Controller:

Category	Data Elements
Account Data	Email address, hashed password, UID, account creation date, account status.
Subscription Data	Subscription tier, entitlements, subscription customer ID. Payment card data is processed solely by third-party payment processors. CyberFence Corp does not store raw payment card data.
Device Data	Device type, OS, app version, registration date. No IP addresses are logged or retained.
Breach Monitor Data	Up to 3 monitored email addresses per account, breach detection results, scan history (rolling 12 months).
Analytics Data	Anonymised, aggregated crash reports and app performance metrics only. No browsing history, DNS queries, or session logs are collected.
Preference Data	Language, theme, notification settings, consent flags.

Data Subjects include: the Controller (where a natural person), and authorized end-users of the Services. CyberFence Corp does not intentionally process special category data (GDPR Article 9). The Controller shall not submit such data to the Services.

3. Processor Obligations

3.1 Instructions Only. CyberFence Corp processes personal data only on the Controller's documented instructions. The Terms of Service and this DPA together constitute those instructions.

3.2 Confidentiality. Personnel authorised to access personal data are bound by confidentiality obligations. Access is restricted to staff who require it to deliver the Services.

3.3 No Sale or Sharing. CyberFence Corp does not sell, rent, or share personal data with any third party for that party's own purposes.

3.4 Zero-Logs Policy. CyberFence Corp does not log or retain: browsing history, DNS queries, connection timestamps, session duration, bandwidth per user, or VPN-assigned IP addresses.

3.5 Compliance Assistance. CyberFence Corp assists the Controller with GDPR Articles 32–36 obligations including security, breach notification, DPIAs, and data subject rights responses.

4. Controller Obligations

4.1 The Controller ensures it has a valid lawful basis under GDPR Article 6 for all personal data submitted to the Services.

4.2 The Controller is responsible for the accuracy and legality of personal data submitted, and for providing appropriate privacy notices to Data Subjects.

4.3 If CyberFence Corp is required by EU or Member State law to process personal data beyond the Controller's instructions, it will inform the Controller before doing so unless prohibited by law.

5. Security (GDPR Article 32)

CyberFence Corp implements appropriate technical and organisational measures including:

- TLS 1.2+ encryption for all data in transit; AES-256 encryption at rest.
- Role-based access controls; MFA required for all production system access.
- Two-factor authentication (TOTP/authenticator app) available for all user accounts.
- Zero-logs VPN architecture — no activity logs are written or stored.
- Incident response procedures and regular security testing.
- Full, irreversible account deletion executed server-side within 24 hours of request.

6. Security Incident Notification

CyberFence Corp notifies the Controller of any confirmed or reasonably suspected personal data breach within 24 hours of becoming aware, enabling the Controller to meet its 72-hour regulatory reporting obligation under GDPR Article 33. Notification includes: nature of the incident, data categories and approximate number of affected Data Subjects, likely consequences, and remediation steps taken.

7. Sub-Processors

7.1 CyberFence Corp engages third-party sub-processors to support the delivery of the Services, including providers of cloud infrastructure, authentication, subscription management, and payment processing. All sub-processors are located in the United States and are bound by data protection obligations at least equivalent to those set out in this DPA. CyberFence Corp remains fully liable to the Controller for the acts and omissions of any sub-processor.

7.2 CyberFence Corp will notify the Controller at least 30 days before adding or replacing a material sub-processor. The Controller may object within 14 days of such notification on data protection grounds by written notice to info@cyberfenceplatform.com.

7.3 The current list of sub-processors is available to the Controller upon written request submitted to info@cyberfenceplatform.com.

8. Data Subject Rights and Deletion

8.1 Rights Assistance. CyberFence Corp assists the Controller in responding to Data Subject requests for access, rectification, erasure, restriction, portability, and objection under GDPR Articles 15–21.

8.2 Account Deletion (Right to Erasure). Upon a verified deletion request, CyberFence Corp permanently and irreversibly deletes all personal data associated with the account, including: authentication credentials, user profile, breach monitoring history, monitored email addresses, and registered device records. Deletion is executed server-side within 24 hours and is irreversible.

8.3 Data Export (Portability). Users can download a machine-readable JSON export of all personal data held via Settings at web.cyberfenceplatform.com.

8.4 Post-Termination. Upon termination, CyberFence Corp deletes or returns all personal data within 30 days at the Controller's election and provides written confirmation of deletion upon request.

9. International Transfers

CyberFence Corp operates exclusively in the United States, which does not benefit from an EU adequacy decision. All transfers of personal data from the EU/EEA to CyberFence Corp are governed by the EU Standard Contractual Clauses — Module 2 (Controller to Processor), adopted under Commission Implementing Decision (EU) 2021/914 of 4 June 2021, incorporated into this DPA by reference. CyberFence Corp confirms it has no reason to believe US law prevents it from fulfilling its obligations under the SCCs and will contest any conflicting government requests through available legal remedies.

10. Audit Rights

CyberFence Corp makes available all information necessary to demonstrate compliance with GDPR Article 28 and this DPA. The Controller may request an audit with 30 days' written notice, no more than once per year (unless a Security Incident has occurred). CyberFence Corp may satisfy audit obligations by providing relevant third-party security reports or certifications within 10 business days of request.

11. Governing Law

This DPA is governed by the laws of the Republic of Ireland. The parties submit to the exclusive jurisdiction of the Irish courts, without prejudice to the Controller's right to lodge a complaint with the competent Supervisory Authority in its EU Member State. The SCCs are governed by Irish law pursuant to Clause 17 thereof.

12. General

12.1 Entire Agreement. This DPA, together with the Terms of Service and the incorporated EU SCCs, constitutes the entire agreement between the parties regarding the processing of personal data.

12.2 Amendments. CyberFence Corp may update this DPA to reflect changes in applicable law. Material changes will be notified to the Controller at least 30 days before taking effect.

12.3 Survival. Sections 6 (Breach Notification), 8 (Deletion), 9 (Transfers), and 10 (Audit) survive termination of this DPA.

Signatures

By signing below, the parties agree to be bound by this Data Processing Agreement and the EU Standard Contractual Clauses (Module 2, June 2021) incorporated herein.

DATA CONTROLLER	DATA PROCESSOR
Legal Entity Name:	Legal Entity Name: CyberFence Corp
Signatory Name: _____	Signatory Name: _____
Title: _____	Title: _____
Signature: _____	Signature: _____
Date: _____	Date: _____
Email: _____	Email: info@cyberfenceplatform.com