

DATA PROCESSING AGREEMENT

pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR)

CyberGuardian XDR

1. Parties

This Data Processing Agreement (the "Agreement") is entered into between:

THE PROCESSOR

CyberGuardian Security EOOD

UIC (EИК): 208647034

Registered office: Sofia, Republic of Bulgaria

Contact: support@cyberguardian.bg

THE CONTROLLER

Company name: _____

Registration number: _____

Registered office: _____

Contact person / email: _____

Each a "Party" and together the "Parties".

2. Subject Matter and Purpose

2.1 The Controller has purchased a subscription to CyberGuardian XDR, an endpoint detection and response solution (the "Service"). In delivering the Service, the Processor processes personal data on behalf of the Controller.

2.2 This Agreement governs that processing and forms an integral part of the Terms of Service accepted by the Controller.

2.3 The purpose of the processing is limited to the provision, operation, security and support of the Service, including threat detection, incident response and compliance reporting.

2.4 In the event of conflict between this Agreement and the Terms of Service in respect of data protection, this Agreement prevails.

3. Duration

This Agreement takes effect on the date of the Controller's subscription activation and remains in force for as long as the Processor processes personal data on behalf of the Controller. Clauses that by their nature survive termination shall continue to apply.

4. Nature of the Processing

4.1 Categories of data subjects:

- Employees, contractors and other authorised users of the Controller's endpoints
- Administrators and account holders designated by the Controller

- Third parties whose data appears in security events, including individuals associated with detected intrusion attempts

4.2 Categories of personal data:

Category	Data processed
Device and status data	Hostname, local IP address, agent version, protection status, resource utilisation
Process and execution data	Process names, executable paths, identifiers, the Windows account under which a process runs, per-process resource usage
Security posture data	Security-relevant system configuration, software inventory, patch and update status, agent integrity status
Detection and incident data	Security events and alerts, quarantine records (file name, hash, action taken), details of detected intrusion attempts including source IP address and port
Account data	Administrator email address, licence key and activation status

4.3 No special categories of personal data within the meaning of Article 9 GDPR are intentionally processed. The Controller shall not configure the Service in a manner that causes such data to be processed.

5. Obligations of the Processor

The Processor shall:

- process personal data only on the documented instructions of the Controller, including this Agreement and the Controller's configuration of the Service, unless required to do otherwise by Union or Member State law;
- ensure that persons authorised to process the personal data are bound by an appropriate obligation of confidentiality;
- implement the technical and organisational measures set out in Annex 1 in accordance with Article 32 GDPR;
- respect the conditions in Clause 7 for engaging sub-processors;
- taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures in responding to requests from data subjects exercising their rights under Chapter III GDPR;
- assist the Controller in ensuring compliance with Articles 32 to 36 GDPR, taking into account the nature of the processing and the information available to the Processor;
- at the choice of the Controller, delete or return all personal data upon termination of the Service, and delete existing copies unless Union or Member State law requires storage;
- make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR and allow for and contribute to audits in accordance with Clause 9;
- immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection provisions.

6. Obligations of the Controller

6.1 The Controller warrants that it has a valid lawful basis for the processing carried out through the Service and that its instructions comply with applicable data protection law.

6.2 Where the Service is deployed on endpoints used by employees or other individuals, the Controller is solely responsible for:

- informing those individuals of the monitoring carried out by the Service in accordance with Articles 13 and 14 GDPR;

- establishing a valid lawful basis for such monitoring under applicable national employment and data protection law;
- completing any works council consultation, employee representative notification or data protection impact assessment required in its jurisdiction.

6.3 The Controller is responsible for the accuracy of the configuration it applies to the Service, including exclusions, retention settings and the scope of monitored endpoints.

7. Sub-processors

7.1 The Controller grants the Processor general authorisation to engage sub-processors, subject to the conditions in this Clause.

7.2 The Processor shall impose on each sub-processor, by written contract, data protection obligations no less protective than those set out in this Agreement, and remains fully liable to the Controller for the performance of each sub-processor's obligations.

7.3 The sub-processors engaged at the date of this Agreement are:

Sub-processor	Purpose	Location
Railway Corp.	Cloud infrastructure and application hosting	European Union (EU West — Amsterdam)
Stripe, Inc.	Payment processing (billing data only) — engaged upon activation of paid subscriptions	European Union / United States — SCCs in place
Resend	Transactional email delivery	European Union
Vercel Inc.	Website hosting and contact form delivery	European Union / United States — SCCs in place

7.4 The Processor shall inform the Controller of any intended addition or replacement of a sub-processor at least thirty (30) days in advance. The Controller may object on reasonable data protection grounds within that period, in which case the Parties shall discuss in good faith; if no resolution is reached, the Controller may terminate the affected part of the Service without penalty.

8. Personal Data Breaches

8.1 The Processor shall notify the Controller without undue delay, and in any event within forty-eight (48) hours, after becoming aware of a personal data breach affecting personal data processed under this Agreement.

8.2 The notification shall describe, to the extent known: the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach.

8.3 The Processor shall cooperate with the Controller and take such reasonable steps as are directed by the Controller to assist in the investigation, mitigation and remediation of the breach. Notification of a breach to the competent supervisory authority under Article 33 GDPR remains the responsibility of the Controller.

9. Audit

9.1 The Processor shall make available to the Controller, upon reasonable written request and no more than once per calendar year, such information as is necessary to demonstrate compliance with this Agreement.

9.2 Where such information is insufficient, the Controller may conduct an audit, or mandate an independent auditor bound by confidentiality, upon thirty (30) days' prior written notice, during normal business hours and in a manner that does not unreasonably disrupt the Processor's operations. The Controller bears the cost of the audit unless it reveals a material breach by the Processor.

9.3 The Processor may satisfy an audit request by providing a current third-party certification or audit report covering the relevant controls.

10. International Transfers

Personal data is processed within the European Union. Where a transfer to a third country is necessary, the Processor shall ensure an appropriate transfer mechanism under Chapter V GDPR, including the Standard Contractual Clauses adopted by the European Commission, and shall inform the Controller in advance.

11. Retention and Deletion

11.1 Personal data is retained only for as long as necessary for the purposes set out in Clause 2, or as required by applicable law.

11.2 Upon termination of the Service, the Processor shall, at the Controller's choice, return or delete all personal data within ninety (90) days, except where retention is required by Union or Member State law or is necessary for the establishment, exercise or defence of legal claims.

12. Liability and Governing Law

12.1 Liability under this Agreement is subject to the limitations set out in the Terms of Service, save where such limitation is not permitted by applicable law.

12.2 This Agreement is governed by the laws of the Republic of Bulgaria. Disputes shall be subject to the jurisdiction of the courts of Sofia, Bulgaria, without prejudice to the rights of data subjects under Articles 79 and 82 GDPR.

Annex 1 — Technical and Organisational Measures

The Processor implements the following measures in accordance with Article 32 GDPR:

Encryption and transmission

- All data transmitted between the endpoint agent and the platform is encrypted in transit using TLS 1.3
- Data at rest is encrypted using AES-256
- Where connectivity is unavailable, data buffered locally on the endpoint is stored in encrypted form

Access control

- Access to production systems is restricted to authorised personnel on a least-privilege basis
- Authentication to the platform uses signed tokens with defined expiry
- Customer data is logically segregated by licence key; access controls prevent cross-tenant access

Confidentiality and integrity

- Input validation and sanitisation applied across all platform endpoints
- Rate limiting applied to protect against abuse and enumeration
- Agent self-protection mechanisms detect and respond to tampering attempts

Availability and resilience

- Automated backups of platform data, stored within the same European Union region, with defined restoration procedures
- The endpoint agent continues to provide local protection independently of platform availability

Testing and assessment

- Regular security testing of the platform, including assessment against the OWASP Top 10
- Vulnerability disclosure programme with a published responsible disclosure policy
- Software supply chain documented through a Software Bill of Materials (SBOM)

Organisational measures

- Personnel with access to personal data are bound by confidentiality obligations
- Documented incident response procedures aligned with NIS2 Article 21 requirements
- Sub-processors assessed prior to engagement and bound by written data protection terms

Signatures

The Parties have executed this Agreement as of the date last signed below.

FOR THE PROCESSOR

Name

Position

Signature

Date

FOR THE CONTROLLER

Name

Position

Signature

Date