CodeSprinter
Innovating today, shaping tomorrow

Security & Privacy Statement

Version 1.0 · 2026

www.codesprinter.net

DOCUMENT

Type · Security & Privacy Statement
Version · 1.0 (2026)
Prepared by · CodeSprinter

CODESPRINTER

Kwikstaartlaan 42
3704 GS Zeist
The Netherlands

CONTACT

info@codesprinter.nl
www.codesprinter.net
Emergency number: 085 - 369 - 7644

COMPANY DETAILS

Chamber of Commerce (KVK) 94394768
VAT NL005081056B55

CHAPTER 1

Introduction and scope

This Security & Privacy Statement describes the technical and organisational measures CodeSprinter takes to protect personal data and client data. It is intended for IT departments, privacy officers and other parties who wish to assess the security approach before or during a collaboration.

CodeSprinter provides software development, management and related services. The measures are tailored to the nature and scale of those services: appropriate, realistic and demonstrable, without claims that cannot be substantiated.

This statement applies to all systems and environments that CodeSprinter manages or uses in carrying out assignments, the software that CodeSprinter develops or maintains on behalf of clients, and the processing of personal data that CodeSprinter carries out as a processor within the meaning of the GDPR. Security and privacy protection are structurally integrated into the services (security and privacy by design): security requirements are taken into account from the outset, personal data is minimised and access is limited to what is strictly necessary. The measures are reviewed periodically.

CHAPTER 2

Infrastructure security

CodeSprinter manages its own server hardware. That hardware is located in a professional colocation data centre in Velbert, Germany, within the EEA. An up-to-date overview of all engaged suppliers is included in the Sub-processor Overview.

This set-up divides responsibility clearly. The data centre provider takes care of the physical environment: access control, camera surveillance, fire protection, redundant power, cooling and network connectivity. CodeSprinter manages the hardware, the operating systems and the applications, and thereby retains full logical control over the data. The data centre provider has no access to the data on the servers; storage is encrypted and the keys remain under CodeSprinter's control.

The server environment consists of multiple nodes. If a node fails, the workload moves to the remaining nodes. For physical repairs, CodeSprinter uses the data centre's remote hands service, so that a faulty disk or power supply can be replaced on site without a trip to the location being necessary.

At network level, environments are shielded by firewalls that allow only the necessary ports and protocols. Administrative access takes place via encrypted SSH connections with key pairs; password authentication is disabled. Unused services and ports are closed. Where applicable, applications are protected by a Web Application Firewall or a comparable measure.

CHAPTER 3

Access management

Access to systems and client data is governed by the principle of minimal access (least privilege). Administrative access is reserved for a fixed, limited group of authorised administrators within CodeSprinter; the rights granted are recorded and reviewed periodically. Access by third parties takes place only after explicit agreement and is documented.

On all platforms where multi-factor authentication (MFA) is available, MFA is enabled and used. This applies to hosting panels, cloud environments, version control systems and e-mail environments. Logging in with a password alone is not permitted for administrator access.

Passwords are managed through a password manager, are not reused and meet current requirements for length and complexity. Access keys (SSH key pairs, API keys, tokens) are created per environment, are not shared between environments, and are revoked immediately upon termination of an assignment or on suspicion of compromise. Default supplier credentials are always changed immediately upon commissioning.

Clients receive access only to the environments and data that relate specifically to them. Login credentials are never shared through unencrypted channels; a secure method is used for this.

CHAPTER 4

Encryption

Encryption is a standard measure in all environments managed by CodeSprinter.

Encryption in transit: all communication between users, applications and servers takes place via TLS (version 1.2 at minimum; TLS 1.3 where the infrastructure supports it). HTTP connections are automatically redirected to HTTPS. TLS certificates are managed through automated infrastructure (such as Let's Encrypt) and renewed in good time. SSH access uses strong key pairs (RSA 4096 or Ed25519 at minimum).

Encryption at rest: disk volumes of production environments are stored encrypted to the extent that the hosting provider supports this. Backups are stored encrypted. Sensitive configuration data (passwords, API keys) is never stored in plain text in source code or version control; environment variables or a secrets management solution are used for this.

CHAPTER 5

Backups and data recovery

Regular and tested backups are a core measure for availability and recovery.

Production environments are backed up automatically every day and the backups are retained for 30 days. Backups are stored at a location separate from the primary production environment, are stored encrypted and are accessible only through the administrator account. The exact frequency and retention period per assignment are recorded in the Backup and Recovery Policy and, where applicable, in the Managed Hosting SLA.

The recoverability of backups is tested periodically: at least once every six months. A backup that has not been tested offers no reliable guarantee. The results of restore tests are documented. If a fault is found, corrective measures are taken immediately. For detailed procedures, CodeSprinter refers to the Backup and Recovery Policy.

CHAPTER 6

Monitoring and logging

The availability and performance of production environments are monitored through automated monitoring. The monitoring runs on CodeSprinter's own infrastructure (Prometheus, Grafana, Uptime Kuma and Sentry). In the event of an outage or a threshold being exceeded, CodeSprinter automatically receives an alert by e-mail and push notification. CodeSprinter does not operate a 24/7 staffed Security Operations Center; the service window runs from Monday to Friday from 08:00 to 20:00, and alerts outside that window are assessed as soon as practically feasible. Critical emergencies can be reported via the emergency number 085 - 369 - 7644.

Servers and applications generate log files of system events, access attempts and errors. Log files are retained for 90 days, are protected against unauthorised modification or deletion, and are kept for administrator sessions so that it can be established afterwards who had access and when. Critical events (repeated failed login attempts, unexpected restarts, disk volumes that are nearly full) generate automatic alerts whose thresholds are reviewed periodically.

CHAPTER 7

Patch and update management

Installing security updates promptly is one of the most effective measures for closing known vulnerabilities. Security updates for the operating system and critical software dependencies are installed as soon as possible after they become available, and in any case within 48 hours of the publication of a critical patch. Non-critical updates are included in a monthly maintenance cycle, with a maximum turnaround time of 30 days. For operating system security updates, CodeSprinter uses automatic installation via unattended-upgrades.

Libraries and frameworks used in developed software are regularly checked for known vulnerabilities using automated dependency management tools. Vulnerable dependencies are updated or replaced as soon as practically feasible. Updates are validated in a test environment before being rolled out to production, unless the urgency of a critical vulnerability requires immediate action.

CHAPTER 8

Secure software development

CodeSprinter integrates security structurally into the development process according to the following principles:

- **Least privilege in code**: applications run with minimal system privileges; database users have only the rights that are necessary.
- **Input validation**: all external input is validated and sanitised to prevent injection attacks (SQL injection, cross-site scripting).
- **No secrets in version control**: passwords, API keys and tokens are never stored in source code or the version control system; environment variables or a secrets management solution are used for this.
- **Dependency management**: external libraries are chosen deliberately and updated regularly.
- **Code review**: code destined for production goes through a review step before it is rolled out.

Development and testing take place in environments separated from production. No real personal data is used in test environments unless technically unavoidable; in that case, data is anonymised or pseudonymised. The full description of the development process and the associated security controls is included in the Secure Development Lifecycle (SDL), which is available on request.

CHAPTER 9

Data segregation

CodeSprinter works for multiple clients. Data segregation ensures that one client's data is not visible or accessible to another client.

Each client has its own, shielded environment (server, container or application instance). Shared environments are not used unless a client explicitly agrees to this and segregation at application level is guaranteed. Databases of different clients are not combined on the same instance, unless logical segregation has been implemented through separate schemas or user accounts with strict access control.

Administrative credentials are unique per environment: a compromised key for environment A does not give access to environment B. Service accounts have no access to data outside their own application domain. Backups per client are stored separately and are not mixed with backups of other clients.

CHAPTER 10

Incident management and data breaches

Despite all precautions, a security incident may occur. A security incident is any event that actually compromises, or may compromise, the confidentiality, integrity or availability of systems or data (unauthorised access, malware, loss of equipment containing client data, a data breach, prolonged unavailability).

Upon suspecting or detecting an incident, CodeSprinter immediately begins investigating and limiting the damage. The affected client(s) are informed as soon as practically feasible about the nature of the incident, the affected systems and the expected consequences.

Where a data breach within the meaning of the GDPR has occurred (a breach leading to the destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data), CodeSprinter informs the controller without undue delay and in any case within 72 hours of discovery. The notification contains at least the nature of the data breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or to be taken. All incidents are recorded in an incident register. The full procedure is described in the Incident and Data Breach Procedure.

CHAPTER 11

Sub-processors

In providing its services, CodeSprinter engages third parties that may process personal data. CodeSprinter engages only sub-processors that provide sufficient guarantees of compliance with the GDPR, and has made contractual arrangements with each sub-processor in line with Article 28 GDPR.

Depending on the assignment, CodeSprinter uses sub-processors in the following categories: the colocation provider that supplies the physical server environment, the backup storage service, the DNS and CDN service, the business e-mail service and the accounting firm. Monitoring and error tracking run on CodeSprinter's own infrastructure and do not involve any external party. An up-to-date, complete overview including name, nature of the processing, place of establishment and any certifications is included in the Sub-processor Overview, which can be requested via info@codesprinter.nl.

CodeSprinter informs clients in advance of intended changes to its list of sub-processors. Clients have the right to object to the engagement of a new sub-processor, in accordance with the Data Processing Agreement.

CHAPTER 12

Data locations

Personal data and client data are stored and processed within the European Economic Area (EEA). Transfer outside the EEA takes place only where a valid legal basis exists under the GDPR (adequacy decision or standard contractual clauses).

- Primary hosting location: own hardware in colocation in Velbert, Germany (within the EEA)
- Backup location: Hetzner Storage Box, Germany (within the EEA)

The exact data locations per assignment are included in the Sub-processor Overview. If a client has specific requirements regarding the storage location (for example, the Netherlands or the EU only), this can be recorded as an additional requirement for the assignment.

CHAPTER 13

Business continuity and availability

CodeSprinter is a compact organisation. To prevent clients from depending on CodeSprinter's availability for the continuity of their environment, the following concrete measures apply:

- **Documentation**: all managed environments, configurations and working methods are documented and kept up to date, so that a client or third party can take over the systems.
- **Transferability**: source code and access details are transferable to the client or a third party designated by the client, in accordance with the Data Processing Agreement, the Statement of Work and the Exit and Handover Document.
- **Backups**: backups are accessible to the client or are handed over on request, so that data recovery does not depend on CodeSprinter's availability.
- **Exit procedure**: upon termination of an assignment or in the event of unforeseen unavailability, the handover is guided by the Exit and Handover Document.
- **Structural source code handover**: instead of source code escrow, the client has continuous access to the repository containing its own source code and documentation throughout the term of the assignment. The source code is therefore available even without CodeSprinter's involvement.

CodeSprinter does not guarantee 24/7 availability, unless this has been separately agreed in a Service Level Agreement. Prolonged reduced availability (for example due to holidays or unforeseen circumstances) may temporarily affect the services. CodeSprinter communicates expected periods of reduced availability proactively. In emergencies, the emergency number 085 - 369 - 7644 is available. For the full analysis, CodeSprinter refers to the BCDR summary and the Exit and Handover Document.

CHAPTER 14

Privacy and GDPR

CodeSprinter processes personal data exclusively as a processor within the meaning of the GDPR, on the written instructions of the client as controller, unless a legal obligation requires otherwise. CodeSprinter does not itself determine the purposes and means of the processing and does not process personal data for its own purposes.

All personal data and client data are treated as strictly confidential. Data is not shared with third parties, other than the engaged sub-processors (see Chapter 11) or where a legal obligation requires it. Requests from data subjects (access, rectification, erasure, portability) received by CodeSprinter are forwarded to the controller; CodeSprinter provides the necessary technical assistance. Personal data is not retained longer than necessary for the performance of the assignment and is deleted or returned upon termination in accordance with the Data Processing Agreement.

The full contractual arrangement is laid down in the Data Processing Agreement. A detailed description of all technical and organisational measures is included in the Technical and Organisational Measures (TOM).

CHAPTER 15

Contact for security and privacy questions

Clients, privacy officers, IT departments and researchers can contact CodeSprinter with questions about information security and privacy.

PRIMARY CONTACT

For all questions about security, privacy, data breaches, audits or this statement:

E-mail: info@codesprinter.nl

CodeSprinter aims to respond to security and privacy questions within two business days.

EMERGENCIES

In the event of a security incident with direct, urgent impact:

Emergency number: 085 - 369 - 7644

This number is intended for emergencies only. Please use the e-mail address for all other questions.

RESPONSIBLE PERSON

Yassine El Fahmi CodeSprinter Kwikstaartlaan 42, 3704 GS Zeist Chamber of Commerce (KVK) 94394768 · VAT NL005081056B55

This statement is reviewed periodically. The most recent version can be requested via info@codesprinter.nl.