CodeSprinter
Innovating today, shaping tomorrow

Security & Privacy Statement

Versie 1.0 · 2026

www.codesprinter.nl

DOCUMENT

Type · Security & Privacy Statement
Versie · 1.0 (2026)
Opgesteld door · CodeSprinter

CODESPRINTER

Kwikstaartlaan 42
3704 GS Zeist
Nederland

CONTACT

info@codesprinter.nl
www.codesprinter.nl
Noodnummer: 085 - 369 - 7644

GEGEVENS

KVK 94394768
BTW NL005081056B55

HOOFDSTUK 1

Inleiding en scope

Dit Security & Privacy Statement beschrijft de technische en organisatorische maatregelen die CodeSprinter neemt om persoonsgegevens en opdrachtgeverdata te beschermen. Het is bestemd voor IT-afdelingen, privacy officers en andere partijen die de beveiligingsaanpak willen beoordelen voorafgaand aan of tijdens een samenwerking.

CodeSprinter levert softwareontwikkeling, beheer en aanverwante diensten. De maatregelen zijn afgestemd op de aard en omvang van die dienstverlening: passend, realistisch en aantoonbaar, zonder claims die niet kunnen worden waargemaakt.

Dit statement is van toepassing op alle systemen en omgevingen die CodeSprinter beheert of gebruikt bij de uitvoering van opdrachten, de software die CodeSprinter ontwikkelt of onderhoudt namens opdrachtgevers, en de verwerking van persoonsgegevens die CodeSprinter uitvoert als verwerker in de zin van de AVG. Beveiliging en privacybescherming worden structureel geïntegreerd in de dienstverlening (security en privacy by design): beveiligingseisen worden van meet af aan meegewogen, persoonsgegevens worden geminimaliseerd en toegang wordt beperkt tot wat strikt noodzakelijk is. De maatregelen worden periodiek herzien.

HOOFDSTUK 2

Infrastructuurbeveiliging

CodeSprinter beheert eigen serverhardware. Die hardware staat in een professioneel colocatie-datacenter in Velbert, Duitsland, binnen de EER. Een actueel overzicht van alle ingeschakelde leveranciers is opgenomen in het Subverwerkersoverzicht.

Deze opzet verdeelt de verantwoordelijkheid helder. De datacenterpartij verzorgt de fysieke omgeving: toegangscontrole, camerabewaking, bescherming tegen brand, redundante stroomvoorziening, koeling en netwerkconnectiviteit. CodeSprinter beheert de hardware, de besturingssystemen en de applicaties, en houdt daarmee de volledige logische controle over de gegevens. De datacenterpartij heeft geen toegang tot de gegevens op de servers; opslag is versleuteld en de sleutels blijven onder beheer van CodeSprinter.

De serveromgeving bestaat uit meerdere nodes. Valt er een node uit, dan verplaatst de werklast zich naar de overige nodes. Voor fysieke reparaties maakt CodeSprinter gebruik van de remote hands-dienst van het datacenter, zodat een defecte schijf of voeding ter plaatse kan worden vervangen zonder dat een reis naar de locatie nodig is.

Op netwerkniveau worden omgevingen afgeschermd via firewalls die uitsluitend noodzakelijke poorten en protocollen toestaan. Beheertoegang verloopt via versleutelde SSH-verbindingen met sleutelparen; wachtwoordauthenticatie is uitgeschakeld. Ongebruikte services en poorten worden gesloten. Waar van toepassing worden applicaties beschermd door een Web Application Firewall of vergelijkbare maatregel.

HOOFDSTUK 3

Toegangsbeheer

Toegang tot systemen en opdrachtgeverdata is geregeld op basis van het principe van minimale toegang (least privilege). Beheertoegang is voorbehouden aan een vaste, beperkte kring van geautoriseerde beheerders binnen CodeSprinter; de toegekende rechten worden vastgelegd en periodiek herzien. Toegang door derden vindt uitsluitend plaats na expliciete afspraak en wordt gedocumenteerd.

Op alle platforms waar meervoudige authenticatie (MFA) beschikbaar is, wordt MFA ingeschakeld en gebruikt. Dit geldt voor hostingpanelen, cloud-omgevingen, versiebeheersystemen en e-mailomgevingen. Aanmelden met uitsluitend een wachtwoord is niet toegestaan voor beheerderstoegang.

Wachtwoorden worden beheerd via een wachtwoordmanager, worden niet hergebruikt en voldoen aan hedendaagse eisen voor lengte en complexiteit. Toegangssleutels (SSH-sleutelparen, API-sleutels, tokens) worden per omgeving aangemaakt, niet gedeeld tussen omgevingen, en bij beëindiging van een opdracht of bij vermoeden van compromittering onmiddellijk ingetrokken. Standaard inloggegevens van leveranciers worden altijd direct gewijzigd bij ingebruikname.

Opdrachtgevers ontvangen uitsluitend toegang tot de omgevingen en data die specifiek op hen betrekking hebben. Inloggegevens worden nooit via onversleutelde kanalen gedeeld; hiervoor wordt een veilige methode gebruikt.

HOOFDSTUK 4

Versleuteling

Versleuteling is een standaardmaatregel in alle omgevingen die CodeSprinter beheert.

Versleuteling onderweg: alle communicatie tussen gebruikers, applicaties en servers verloopt via TLS (minimaal versie 1.2; TLS 1.3 waar de infrastructuur dit ondersteunt). HTTP-verbindingen worden automatisch doorgestuurd naar HTTPS. TLS-certificaten worden via geautomatiseerde infrastructuur (zoals Let's Encrypt) beheerd en tijdig vernieuwd. SSH-toegang maakt gebruik van sterke sleutelparen (minimaal RSA 4096 of Ed25519).

Versleuteling in rust: schijfvolumes van productieomgevingen worden versleuteld opgeslagen voor zover de hostingprovider dit ondersteunt. Back-ups worden versleuteld opgeslagen. Gevoelige configuratiegegevens (wachtwoorden, API-sleutels) worden nooit in platte tekst opgeslagen in broncode of versiebeheer; hiervoor worden omgevingsvariabelen of een secrets-beheeroplossing gebruikt.

HOOFDSTUK 5

Back-ups en gegevensherstel

Regelmatige en geteste back-ups zijn een kernmaatregel voor beschikbaarheid en herstel.

Productieomgevingen worden dagelijks automatisch geback-upt en de back-ups worden 30 dagen bewaard. Back-ups worden opgeslagen op een locatie die is gescheiden van de primaire productieomgeving, worden versleuteld opgeslagen en zijn uitsluitend toegankelijk via de beheerdersaccount. De exacte frequentie en retentie per opdracht worden vastgelegd in het Backup- en herstelbeleid en, waar van toepassing, in de Managed Hosting SLA.

De herstelbaarheid van back-ups wordt periodiek getest: ten minste eenmaal per half jaar. Een back-up die niet is getest, biedt geen betrouwbare garantie. Uitkomsten van hersteltests worden gedocumenteerd. Bij constatering van een fout worden direct correctieve maatregelen genomen. Voor gedetailleerde procedures verwijst CodeSprinter naar het Backup- en herstelbeleid.

HOOFDSTUK 6

Monitoring en logging

Beschikbaarheid en prestaties van productieomgevingen worden bewaakt via geautomatiseerde monitoring. De monitoring draait op de eigen infrastructuur (Prometheus, Grafana, Uptime Kuma en Sentry). Bij een storing of drempeloverschrijding ontvangt CodeSprinter automatisch een melding per e-mail en pushbericht. CodeSprinter beheert geen 24/7-bemand Security Operations Center; het servicevenster loopt van maandag tot en met vrijdag van 08:00 tot 20:00, en meldingen buiten dat venster worden beoordeeld zodra dat praktisch haalbaar is. Kritieke noodsituaties kunnen worden gemeld via het noodnummer 085 - 369 - 7644.

Servers en applicaties genereren logbestanden van systeemgebeurtenissen, toegangspogingen en fouten. Logbestanden worden bewaard gedurende 90 dagen, zijn beschermd tegen ongeautoriseerde wijziging of verwijdering, en worden bijgehouden voor beheerderssessies zodat achteraf kan worden vastgesteld wie wanneer toegang heeft gehad. Kritieke gebeurtenissen (herhaalde mislukte inlogpogingen, onverwachte herstarts, schijfvolumes die bijna vol zijn) genereren automatische meldingen waarvan de drempelwaarden periodiek worden beoordeeld.

HOOFDSTUK 7

Patch- en updatebeheer

Het tijdig installeren van beveiligingsupdates is een van de meest effectieve maatregelen om bekende kwetsbaarheden te dichten. Beveiligingsupdates voor het besturingssysteem en kritieke software-afhankelijkheden worden zo spoedig mogelijk na beschikbaarheid geïnstalleerd, en in elk geval binnen 48 uur na publicatie van een kritieke patch. Niet-kritieke updates worden meegenomen in een maandelijkse onderhoudscyclus, met een maximale doorlooptijd van 30 dagen. Voor beveiligingsupdates van het besturingssysteem maakt CodeSprinter gebruik van automatische installatie via unattended-upgrades.

Bibliotheken en frameworks die worden gebruikt in ontwikkelde software worden regelmatig gecontroleerd op bekende kwetsbaarheden via geautomatiseerde tools voor afhankelijkheidsbeheer. Kwetsbare afhankelijkheden worden zo snel als praktisch haalbaar bijgewerkt of vervangen. Updates worden in een testomgeving gevalideerd voordat ze op productie worden doorgevoerd, tenzij de urgentie van een kritieke kwetsbaarheid directe actie vereist.

HOOFDSTUK 8

Veilige softwareontwikkeling

CodeSprinter integreert beveiliging structureel in het ontwikkelproces volgens de volgende principes:

- **Least privilege in code**: applicaties draaien met minimale systeemrechten; databasegebruikers hebben alleen de rechten die noodzakelijk zijn.
- **Invoervalidatie**: alle invoer van buitenaf wordt gevalideerd en gesaneerd om injectieaanvallen (SQL-injectie, cross-site scripting) te voorkomen.
- **Geen geheimen in versiebeheer**: wachtwoorden, API-sleutels en tokens worden nooit opgeslagen in broncode of het versiebeheersysteem; hiervoor worden omgevingsvariabelen of een secrets-beheeroplossing gebruikt.
- **Afhankelijkheidsbeheer**: externe bibliotheken worden bewust gekozen en regelmatig bijgewerkt.
- **Code review**: code voor productie doorloopt een reviewstap voordat deze wordt uitgerold.

Ontwikkeling en testen vinden plaats in omgevingen die zijn gescheiden van productie. In testomgevingen worden geen echte persoonsgegevens gebruikt tenzij technisch onvermijdelijk; in dat geval worden gegevens geanonimiseerd of gepseudonimiseerd. De volledige beschrijving van het ontwikkelproces en de bijbehorende beveiligingscontroles is opgenomen in de Secure Development Lifecycle (SDL), die op verzoek beschikbaar is.

HOOFDSTUK 9

Datascheiding

CodeSprinter werkt voor meerdere opdrachtgevers. Datascheiding zorgt ervoor dat gegevens van de ene opdrachtgever niet zichtbaar of toegankelijk zijn voor een andere opdrachtgever.

Elke opdrachtgever beschikt over een eigen, afgeschermde omgeving (server, container of applicatie-instantie). Gedeelde omgevingen worden niet gebruikt tenzij een opdrachtgever hier expliciet mee instemt en scheiding op applicatieniveau is gewaarborgd. Databases van verschillende opdrachtgevers worden niet gecombineerd op dezelfde instantie, tenzij logische scheiding is geïmplementeerd via afzonderlijke schema's of gebruikersaccounts met strikte toegangscontrole.

Beheerreferenties zijn per omgeving uniek: een gecompromitteerde sleutel voor omgeving A geeft geen toegang tot omgeving B. Serviceaccounts hebben geen toegang tot data buiten hun eigen applicatiedomein. Back-ups per opdrachtgever worden afzonderlijk opgeslagen en zijn niet gemengd met back-ups van andere opdrachtgevers.

HOOFDSTUK 10

Incidentbeheer en datalekken

Ondanks alle voorzorgsmaatregelen kan een beveiligingsincident optreden. Een beveiligingsincident is elke gebeurtenis die de vertrouwelijkheid, integriteit of beschikbaarheid van systemen of gegevens daadwerkelijk aantast of kan aantasten (ongeautoriseerde toegang, malware, verlies van apparatuur met opdrachtgeverdata, een datalek, langdurige onbeschikbaarheid).

Bij het vermoeden of constateren van een incident start CodeSprinter onmiddellijk met het onderzoeken en beperken van de schade. De getroffen opdrachtgever(s) worden zo snel als praktisch haalbaar geïnformeerd over de aard, de getroffen systemen en de te verwachten gevolgen.

Indien sprake is van een datalek in de zin van de AVG (een inbreuk die leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking van of ongeoorloofde toegang tot persoonsgegevens), informeert CodeSprinter de verwerkingsverantwoordelijke zonder onnodige vertraging en in elk geval binnen 72 uur na ontdekking. De melding bevat ten minste de aard van het datalek, de categorieën en het geschatte aantal betrokkenen en records, de waarschijnlijke gevolgen, en de genomen of te nemen maatregelen. Alle incidenten worden geregistreerd in een incidentregister. De volledige procedure is beschreven in de Incident- en datalekprocedure.

HOOFDSTUK 11

Subverwerkers

Voor de uitvoering van de dienstverlening schakelt CodeSprinter derde partijen in die persoonsgegevens kunnen verwerken. CodeSprinter schakelt uitsluitend subverwerkers in die afdoende garanties bieden voor de naleving van de AVG, en heeft met elke subverwerker contractuele afspraken gemaakt in lijn met artikel 28 AVG.

Afhankelijk van de opdracht maakt CodeSprinter gebruik van subverwerkers in de volgende categorieën: de colocatie-partij die de fysieke serveromgeving levert, de back-upopslagdienst, de DNS- en CDN-dienst, de zakelijke e-maildienst en het administratiekantoor. Monitoring en foutregistratie draaien op de eigen infrastructuur en betrekken geen externe partij. Een actueel, volledig overzicht inclusief naam, aard van de verwerking, vestigingslocatie en eventuele certificeringen is opgenomen in het Subverwerkersoverzicht, op te vragen via info@codesprinter.nl.

CodeSprinter stelt opdrachtgevers vooraf op de hoogte van beoogde wijzigingen in het subverwerkersbestand. Opdrachtgevers hebben het recht bezwaar te maken tegen de inschakeling van een nieuwe subverwerker, overeenkomstig de Verwerkersovereenkomst.

HOOFDSTUK 12

Datalocaties

Persoonsgegevens en opdrachtgeverdata worden opgeslagen en verwerkt binnen de Europese Economische Ruimte (EER). Doorgifte buiten de EER vindt alleen plaats als daarvoor een geldige rechtsgrond bestaat op grond van de AVG (adequaatheidsbesluit of standaardcontractbepalingen).

- Primaire hostinglocatie: eigen hardware in colocatie te Velbert, Duitsland (binnen de EER)
- Back-uplocatie: Hetzner Storage Box, Duitsland (binnen de EER)

De exacte datalocaties per opdracht zijn opgenomen in het Subverwerkersoverzicht. Indien een opdrachtgever specifieke vereisten heeft ten aanzien van de opslaglocatie (bijvoorbeeld uitsluitend Nederland of de EU), kan dit als aanvullende eis worden vastgelegd bij de opdracht.

HOOFDSTUK 13

Bedrijfscontinuïteit en beschikbaarheid

CodeSprinter is een compacte organisatie. Om te voorkomen dat opdrachtgevers voor de continuïteit van hun omgeving afhankelijk zijn van de beschikbaarheid van CodeSprinter, gelden de volgende concrete maatregelen:

- **Documentatie**: alle beheerde omgevingen, configuraties en werkwijzen worden actueel gedocumenteerd, zodat een opdrachtgever of derde de systemen kan overnemen.
- **Overdraagbaarheid**: broncode en toegangsgegevens zijn overdraagbaar aan de opdrachtgever of een door de opdrachtgever aangewezen derde, overeenkomstig de Verwerkersovereenkomst, de Opdrachtbevestiging en het Exit- en overdrachtsdocument.
- **Back-ups**: back-ups zijn toegankelijk voor de opdrachtgever of worden op verzoek overgedragen, zodat gegevensherstel niet afhankelijk is van de beschikbaarheid van CodeSprinter.
- **Exit-procedure**: bij beëindiging van een opdracht of bij onvoorziene uitval wordt de overdracht begeleid via het Exit- en overdrachtsdocument.
- **Structurele broncode-overdracht**: in plaats van broncode-escrow heeft de opdrachtgever gedurende de looptijd van de opdracht doorlopend toegang tot de repository met zijn eigen broncode en documentatie. De broncode is daarmee ook zonder tussenkomst van CodeSprinter beschikbaar.

CodeSprinter garandeert geen 24/7-bereikbaarheid, tenzij dit in een Service Level Agreement afzonderlijk is vastgelegd. Langdurige verminderde beschikbaarheid (bijvoorbeeld door vakantie of onvoorziene omstandigheden) kan de dienstverlening tijdelijk beïnvloeden. CodeSprinter communiceert verwachte perioden van verminderde beschikbaarheid proactief. In noodgevallen is het noodnummer 085 - 369 - 7644 bereikbaar. Voor de volledige analyse verwijst CodeSprinter naar de BCDR-samenvatting en het Exit- en overdrachtsdocument.

HOOFDSTUK 14

Privacy en AVG

CodeSprinter verwerkt persoonsgegevens uitsluitend als verwerker in de zin van de AVG, op schriftelijke instructie van de opdrachtgever als verwerkingsverantwoordelijke, tenzij een wettelijke verplichting anders vereist. CodeSprinter bepaalt niet zelf het doel van en de middelen voor de verwerking en verwerkt persoonsgegevens niet voor eigen doeleinden.

Alle persoonsgegevens en opdrachtgeverdata worden behandeld als strikt vertrouwelijk. Gegevens worden niet gedeeld met derden, behoudens de ingeschakelde subverwerkers (zie Hoofdstuk 11) of wanneer een wettelijke verplichting dat vereist. Verzoeken van betrokkenen (inzage, correctie, verwijdering, overdraagbaarheid) die bij CodeSprinter binnenkomen, worden doorgestuurd naar de verwerkingsverantwoordelijke; CodeSprinter verleent de benodigde technische medewerking. Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de uitvoering van de opdracht en na beëindiging verwijderd of teruggegeven overeenkomstig de Verwerkersovereenkomst.

De volledige contractuele regeling is vastgelegd in de Verwerkersovereenkomst. Een gedetailleerde beschrijving van alle technische en organisatorische maatregelen is opgenomen in de Technische en Organisatorische Maatregelen (TOM).

HOOFDSTUK 15

Contact voor security- en privacyvragen

Opdrachtgevers, privacy officers, IT-afdelingen en onderzoekers kunnen voor vragen over informatiebeveiliging en privacy contact opnemen met CodeSprinter.

PRIMAIR CONTACT

Voor alle vragen over beveiliging, privacy, datalekken, audits of dit statement:

E-mail: info@codesprinter.nl

CodeSprinter streeft ernaar op beveiligings- en privacyvragen te reageren binnen twee werkdagen.

NOODGEVALLEN

Bij een beveiligingsincident met directe, urgente impact:

Noodnummer: 085 - 369 - 7644

Dit nummer is uitsluitend bestemd voor noodgevallen. Gebruik voor alle overige vragen het e-mailadres.

VERANTWOORDELIJKE

Yassine El Fahmi CodeSprinter Kwikstaartlaan 42, 3704 GS Zeist KVK 94394768 · BTW NL005081056B55

Dit statement wordt periodiek herzien. De meest actuele versie is op te vragen via info@codesprinter.nl.