Richtlijnen Cloudapplicaties

Leidraad 2026

1 Algemeen

Tegenwoordig worden meer en meer applicaties in de cloud beheerd. Vanuit een beheers-optiek lijkt dat handig, en daarom kopen veel MBO instellingen hierop in. Zo ook Aventus.

Maar cloud toepassingen hebben een aantal belangrijke keerzijdes. Het feit dat ze buiten de muren van Aventus huizen maakt dat beveiliging van groot belang is. Alle gegevens die in de cloud terecht komen, staan ‘buiten de deur’ en worden door externen beheerd. Toch blijft Aventus ten alle tijden verantwoordelijk.

Dit document beschrijft de minimumeisen voor veilige, privacy-conforme en soevereine clouddiensten.

Herziene versie, Mei 2026

2 Inhoudsopgave

3 Algemeen en toepassingsbereik

Dit document stelt eisen aan de hosting, beveiliging, privacy en gegevensbeschikking van cloudapplicaties die worden aanbesteed of ingekocht. De eisen zijn van toepassing op alle vormen van extern beheerde software en infrastructuur, waaronder:

- Software as a Service (SaaS) — de leverancier beheert applicatie én infrastructuur.
- Managed hosting — de leverancier beheert de infrastructuur; de applicatie kan eigen ontwikkeling zijn.
- Integration Platform as a Service (iPaaS) — de leverancier levert een integratieplatform waarop koppelingen tussen systemen worden uitgevoerd.
- Platform as a Service (PaaS) — de leverancier levert een platform waarop de Opdrachtgever eigen applicaties draait.

Voor de API-koppelingen die vanuit of naar een aanbesteed systeem lopen, gelden aanvullende eisen die zijn beschreven in het document “API Richtlijnen”. Beide documenten zijn complementair en dienen samen te worden gehanteerd bij aanbestedingen waarbij een extern systeem via een API gegevens uitwisselt met het integratieplatform van de Opdrachtgever.

✦ Aanbestedingseis
De Inschrijver verklaart bij inschrijving dat het aangeboden systeem voldoet aan alle eisen in dit document. Afwijkingen worden expliciet vermeld met een beschrijving van de alternatieve maatregel. De Inschrijver geeft ook aan onder welke leveringsvorm (SaaS, managed hosting, iPaaS, PaaS) het aanbod valt, zodat de toepasselijkheid van de eisen correct kan worden beoordeeld.

4 Beveiliging

Omdat cloudapplicaties niet intern staan worden hoge eisen gesteld aan beveiliging. De eisen in deze sectie gelden voor de volledige gehoste omgeving, inclusief onderliggende infrastructuur en diensten van derden

4.1 Gebruikelijke maatregelen

- **Poortenbeleid.** Alleen relevante poorten worden beschikbaar gesteld aan de buitenwereld. Waar mogelijk worden geen standaard poortnummers gebruikt, uitgezonderd HTTP/HTTPS.
- **Patchbeleid (eis).** Beveiligingspatches en updates worden binnen 72 uur na beschikbaarheid toegepast voor kritieke kwetsbaarheden (CVSS ≥9.0), en binnen 30 dagen voor overige patches. De leverancier rapporteert maandelijks de patchstatus aan de Opdrachtgever.
- **Certificaatbeheer (eis).** De leverancier heeft aantoonbaar certificaatbeheer ingericht. Certificaten worden vernieuwd vóór de vervaldatum. Verlopen certificaten zijn een serieuze tekortkoming.
- **DDoS en ransomware.** Aantoonbare maatregelen zijn getroffen tegen DDoS- en ransomware-aanvallen.
- **Geografische toegangsbeperking.** Verkeer afkomstig uit bekende risicogebieden buiten de EU is beperkt of geblokkeerd. De leverancier documenteert welke regio's geblokkeerd zijn en op welke technische grondslag.
- **Server-headers.** Systemen communiceren in de host-header (Server-header element) niet welke software en versie wordt gebruikt. Deze header wordt weggelaten of geanonimiseerd om informatielekken naar aanvallers te voorkomen.

4.2 Communicatiebeveiliging

- **SSL/TLS verplicht.** Al het verkeer van en naar de cloudapplicatie is SSL-versleuteld (HTTPS, minimaal TLS 1.2). Self-signed certificaten zijn niet toegestaan; de leverancier gebruikt certificaten van een officiële Certificate Authority.
- **Encryptie bij afwijkend protocol.** Als het transportprotocol geen SSL-mogelijkheden biedt, wordt de data versleuteld met minimaal AES-256 of sterker.
- **Fysiek transport.** Bij fysiek transport van gevoelige data tijdens migraties (bijvoorbeeld via USB of externe schijven) is de data op het transportmedium versleuteld conform actuele encryptiestandaarden (bijv. VeraCrypt of equivalent).

- **Invoervalidatie.** Bij in- en uitvoer van data worden normalisatie, validatie en inperking toegepast ter bescherming tegen injectieaanvallen (SQL-injectie, XSS e.d.).

✦ Aanbestedingseis
De Inschrijver beschrijft in de inschrijving het patchbeleid (responstijden per CVSS-klasse), het certificaatbeheerproces en de gehanteerde DDoS-mitigatiemaatregelen.

5 3. Toegangsbeveiliging en autorisaties

5.1 Authenticatie

- **Federatieve authenticatie (eis).** Applicaties maken gebruik van SAML 2.0 of OpenID Connect voor identificatie en authenticatie via SurfConext of Kennisnet. Lokale gebruikers logins zijn niet toegestaan voor eindgebruikers. Via SurfConext kan MFA worden afgedwongen.
- **Microsoft Entra / Azure AD niet als centrale IDP.** Microsoft AD/Azure AD/Entra is niet de centrale identity provider van de Opdrachtgever en is dus niet de wijze om Single-Sign-On te realiseren.
- **Persoonlijke beheerdersaccounts (eis).** Ontwikkelaars en beheerders gebruiken uitsluitend persoonlijke accounts. Gedeelde ‘admin’- of ‘god mode’-accounts die door meerdere personen worden gebruikt zijn niet toegestaan.
- **Gescheiden credentials op Test, Acceptatie en productie.** Beheerders en API koppelingen hebben gescheiden credentials op de test, acceptatie en productie instanties.

5.2 Autorisaties

- **Rol gebaseerde autorisaties.** Het systeem kan autorisaties geautomatiseerd toepassen op basis van een rol en/of specialisatiekenmerk van een account. (RBAC) Dit is een pre bij beoordeling.
- **Rolkoppeling.** Een account kan aan één of meerdere rollen worden gekoppeld.
- **Direct effect bij rolwijziging.** Als autorisaties van een rol worden verwijderd, zijn deze direct bij alle accounts met die rol verwijderd — zonder handmatige actie per account.
- **Einddatum op autorisaties.** Het is een pre als aan een autorisatie een einddatum of termijn kan worden meegegeven, zodat tijdelijke toegang automatisch verloopt.
- **API voor autorisatiebeheer.** Als autorisaties niet door het systeem zelf kunnen worden gezet op basis van de rol, is het een pre dat hiervoor een API beschikbaar is. De eisen voor die API staan in het document “API Richtlijnen”.

✦ Aanbestedingseis
De Inschrijver beschrijft de ondersteunde federatieve authenticatiemethode (SAML 2.0 / OIDC) en de wijze waarop rol gebaseerde autorisaties worden ingericht en gesynchroniseerd.

6 Privacy en AVG

Als persoonsgegevens worden verwerkt in een cloudapplicatie gelden aanvullende eisen. Persoonsgegevens zijn alle gegevens over een persoon: ook naam, geslacht, leeftijd, foto, voortgang, score of foto.

6.1 Verwerkersovereenkomst (eis)

De leverancier sluit bij contractsluiting een AVG-conforme verwerkersovereenkomst met de Opdrachtgever. Deze overeenkomst:

- Beschrijft exact welke gegevens worden verwerkt;
- Beschrijft per gegeven de verwerkingsgrondslag en het doel (doelbinding);
- Beschrijft waar en hoe lang gegevens worden opgeslagen;
- Verklaart dat gegevens uitsluitend ten behoeve van de Opdrachtgever worden verwerkt;
- Bevat een actueel register van alle sub verwerkers; wijzigingen worden minimaal 30 dagen van tevoren gecommuniceerd.

6.2 Bijzondere persoonsgegevens

Bijzondere persoonsgegevens zijn (BSN, gezondheidsgegevens, politieke opvattingen, strafverleden, relaties, ECK-iD, geheim adres, beschermingsstatus). Hiervoor gelden aanvullende strengere eisen.

- **Minimale opslag.** Bijzondere persoonsgegevens worden alleen opgeslagen als dit strikt noodzakelijk is en expliciet is verklaard waarom. De reden is aantoonbaar proportioneel. Bij voorkeur worden dergelijke gegevens ‘just-in time’ opgevraagd en niet langer opgeslagen dan strikt noodzakelijk.
- **Aanvullende encryptie.** Bij opslag van bijzondere persoonsgegevens (zoals BSN of ECK-id) kunnen aanvullende encryptie-eisen en is separate opslag gelden.
- **Data-minimalisatie.** Alleen informatie die echt nodig is voor de verwerkingsdoeleinden wordt opgeslagen. Meer data bewaren dan strikt noodzakelijk is niet toegestaan en kan in geval van een datalek leiden tot vergoedingsplicht voor de schade.
- **Log uitsluiting.** Bijzondere persoonsgegevens worden uitgesloten van alle logs en niet inhoudelijk getoond bij foutmeldingen.

6.3 Bewaartermijnen

- **Geautomatiseerde opschoning (eis).** De software is in staat gegevens geautomatiseerd periodiek op te schonen conform wettelijke bewaartermijnen. De termijn is per soort gegeven instelbaar door de Opdrachtgever. Mocht blijken dat de opschoning niet conform de ingestelde parameters werkt, dan kan dit in geval van een datalek leiden tot vergoedingsplicht voor de schade.
-

6.4 Datalocatie (eis)

- **Verwerking binnen Nederland (gunningvoorkeur).** Gegevens — niet alleen persoonsgegevens — worden bij voorkeur verwerkt en opgeslagen in Nederland. Dit levert punten op bij de kwalitatieve beoordeling.
- **Verwerking binnen de EU (eis).** De leverancier garandeert dat gegevens in geen geval buiten de EU/EER worden verwerkt of opgeslagen, ook niet door haar technisch personeel. De leverancier toont dit aantoonbaar aan, bijvoorbeeld via een sub verwerkers-register en datacenter-certificering.

Aanvullende eisen met betrekking tot jurisdictie, CLOUD Act-risico's en digitale soevereiniteit zijn uitgewerkt in sectie 5.

> ✦ **Aanbestedingseis**
> Eis: de Inschrijver levert bij inschrijving een concept-verwerkersovereenkomst met sub-verwerkers-register en toont aan op welke wijze EU-verwerking is geborgd (datacenter-locaties, certificering).

7 Digitale soevereiniteit en jurisdictie

Fysieke hosting binnen de EER is een noodzakelijke maar niet voldoende voorwaarde voor digitale soevereiniteit. Wetgeving zoals de CLOUD Act (Clarifying Lawful Overseas Use of Data Act, 2018) geeft Amerikaanse autoriteiten het recht geven om data op te vragen bij bedrijven die onder Amerikaanse jurisdictie vallen — ongeacht waar die data fysiek staat, zonder dat dit gemeld wordt. Eenzelfde risico ontstaat bij een gedwongen overname, faillissement of sanctie van een toeleverancier in de stack.

7.1 EER-wetgeving op de volledige stack (eis)

- **Nederlandse wetgeving prevaleert.** Op de gehele gehoste omgeving — inclusief onderliggende componenten, sub verwerkers en diensten van derden — is de EER-wetgeving van kracht. De Nederlandse wetgeving prevaleert boven die van externe mogendheden. De leverancier borgt dit contractueel richting alle sub verwerkers.
- **Hosting binnen de EER (eis).** De volledige omgeving — inclusief eventuele CDN nodes, API-gateways, monitoring- en logging-infrastructuur die persoonsgegevens verwerken — is fysiek gehost binnen de EER. Dit is aantoonbaar via het sub verwerkers-register.
- **Jurisdictietransparantie per stack-laag (eis).** De Inschrijver documenteert per laag van de technische stack (hosting, CDN, identity provider, monitoring, betaalinfrastructuur, ticketing-systeem) de juridische vestigingsplaats en nationaliteit van de eigenaar. Componenten die onder niet-EER jurisdictie vallen worden expliciet benoemd, inclusief de bijbehorende mitigerende maatregelen. Indien componenten niet in EER jurisdictie kunnen vallen is de Inschrijver verplicht om elk jaar de onderzoeken of dit nog gegrond is en rapporteert hier jaarlijks schriftelijk over. Mocht blijken dat de componenten inmiddels toch binnen de EER jurisdictie kunnen vallen is een actieve inspanning van de Inschrijver vereist om deze componenten een redelijke termijn alsnog onder EER jurisdictie te brengen.

7.2 Mitigatie van extraterritoriale wetgeving (eis indien niet-EER componenten aanwezig)

- **Sleutelbeheer bij de Opdrachtgever.** Voor componenten die onder niet-EER jurisdictie vallen toont de Inschrijver aan dat persoonsgegevens end-to-end versleuteld zijn met sleutels die uitsluitend in beheer zijn van de Opdrachtgever of een door de Opdrachtgever aangewezen EER-entiteit. Een CLOUD Act-verzoek aan de leverancier levert in dit scenario geen leesbare persoonsgegevens op.
- **Contractuele doorzettingsmacht.** De leverancier legt in zijn contracten met niet-EER sub verwerkers vast dat verzoeken van buitenlandse autoriteiten tot gegevensverstrekking worden bestreden en onverwijld gemeld aan de Opdrachtgever, voor zover wettelijk toegestaan.

7.3 Change of control — meldplicht en opzeggingsrecht (eis)

- **Meldplicht bij eigendomswijziging.** De leverancier informeert de Opdrachtgever schriftelijk en zo vroeg mogelijk, maar uiterlijk 90 dagen voor voltooiing, over een aanstaande verkoop, fusie, overname of andere eigendomswijziging van de leverancier zelf of van een wezenlijk onderdeel van de technische stack. Onder ‘wezenlijk’ wordt verstaan: elk onderdeel zonder welk de dienstverlening niet kan voortgaan.
- **Boetevrij opzeggingsrecht.** De Opdrachtgever heeft het recht de overeenkomst zonder boete en met een opzegtermijn van 1 jaar te beëindigen indien een change of control leidt tot: (a) een nieuwe eigenaar of moedermaatschappij gevestigd buiten de EER, (b) onderwerping aan wetgeving die extraterritoriale toegang tot persoonsgegevens mogelijk maakt, of (c) een situatie die de Opdrachtgever anderszins als onacceptabel beoordeelt voor de digitale soevereiniteit. Dit recht vervalt niet als de wijziging buiten de wil van de leverancier plaatsvindt.

7.4 Volledig soevereine aanbieding — gunningvoorkeur

De Opdrachtgever erkent dat volledige digitale soevereiniteit voor niet alle leveranciers haalbaar is. Tegelijkertijd is het een expliciet beleidsdoel. Aanbiedingen die aantoonbaar volledig soeverein zijn genieten een voorkeur bij de kwalitatieve gunningsbeoordeling.

Een aanbieding is volledig soeverein indien aan álle volgende criteria is voldaan:

- De Inschrijver en alle sub-verwerkers zijn rechtspersonen die uitsluitend binnen de EER zijn gevestigd.
- Geen enkele component van de technische stack is eigendom van, of juridisch onderworpen aan, een entiteit buiten de EER. Open Source componenten worden in dit verband als soeverein gezien.
- De volledige stack valt juridisch uitsluitend onder EER-wetgeving; geen enkele laag is onderworpen aan extraterritoriale wetgeving van derde landen (zoals de CLOUD Act, FISA of vergelijkbare wetgeving).
- De Inschrijver kan dit aantonen via een verklaring van een onafhankelijke EER-accountant of via een erkend soevereiniteitskeurmerk (zoals een EU Cloud Certification Scheme onder ENISA).

Inschrijvers die niet volledig soeverein zijn maar wel voldoen aan alle eisen in 5.1 t/m 5.3 zijn onverminderd ontvankelijk.

✦ **Aanbestedingseis**

Eis (5.1–5.3): de Inschrijver levert bij inschrijving:

a) een stackoverzicht met juridische jurisdictie per laag;

b) een beschrijving van mitigerende maatregelen voor niet-EER componenten (indien van toepassing);

c) bevestiging van de change of control clausule en het boetevrije opzeggingsrecht.

✦ **Voorkeur – volledig soeverein**

Gunningvoorkeur (5.4): de Inschrijver geeft aan of de aanbieding als volledig soeverein kan worden gekwalificeerd en levert het vereiste bewijs (accountantsverklaring of keurmerk).

8 LOG en Audit

8.1 Logging

Systemen houden een applicatielog bij. De Opdrachtgever kan op verzoek inzage krijgen in de log op minimaal Error-niveau. Logs bevatten geen bijzondere persoonsgegevens.

Loggegevens worden geroteerd: informatie van oudere datum wordt overschreven na 1 maand doorlooptijd.

8.2 Auditlog

Naast de applicatielog wordt een auditlog bijgehouden. Hierin staat wie wanneer toegang heeft gehad tot het systeem of bijzondere persoonsgegevens. De auditlog bevat minimaal: datum/tijd, account, host-header en IP-adres van de inlog. Verwerking via een API-gateway is toegestaan.

- **Beschikbaarheid (eis).** De auditlog is op eerste verzoek van de Opdrachtgever beschikbaar, met een minimale bewaartermijn van 6 maanden.
- **Geen bijzondere persoonsgegevens in standaard logregels.** Bijzondere persoonsgegevens worden niet opgenomen in standaard loglevel-regels. Alleen in debug-modus — tijdelijk en na expliciete goedkeuring van de Opdrachtgever — mag de volledige context worden gelogd.

8.3 Maintenancelog

Wijzigingen aan het systeem — updates, patches, herstarts, her configuratie van toegangsparameters (inclusief API-integraties) — worden bijgehouden in een maintenancelog. Deze log is online opvraagbaar. Het niet actueel houden hiervan is een serieuze tekortkoming.

9 Omgevingen

De Opdrachtgever werkt met meerdere omgevingen om applicaties en integraties te gebruiken en testen. De leverancier stelt voor elke onderstaande omgeving een equivalent beschikbaar.

9.1 Testomgeving

De testomgeving is bedoeld om te oefenen en/of een configuratie te testen. Deze omgeving bevat geen herleidbare persoonsgegevens en is niet gekoppeld aan de buitenwereld of andere productiesystemen.

9.2 Acceptatieomgeving

De acceptatieomgeving is een functionele kopie van de productieomgeving, maar lichter uitgevoerd. Deze omgeving bevat koppelingen naar de acceptatieversies van andere systemen in het systeemlandschap.

Periodiek kunnen gegevens van de productieomgeving worden overgezet. Bijzondere persoonsgegevens worden daarbij gerandomiseerd. E-mailadressen en telefoonnummers worden gewijzigd zodat ze niet bruikbaar zijn. Configuratiedefinities voor koppelingen met andere systemen worden bij overzetting niet meegenomen.

9.3 Productieomgeving

De productieomgeving is volledig ingericht conform de afgesloten SLA: uptime, schaalbaarheid, back-ups en onderhoudsvensters. De Opdrachtgever wordt altijd betrokken bij issues of aanpassingen aan integraties met andere systemen.

10 Gegevensbeschikking en exit

De Opdrachtgever is en blijft te allen tijde verantwoordelijk voor alle gegevens die worden verwerkt. Los van de continuïteitsmaatregelen in de SLA moet de Opdrachtgever te allen tijde over deze gegevens kunnen beschikken.

- **Back-up op afroep.** De Opdrachtgever kan op afroep beschikken over de meest recente back-up, zowel online als op een offline medium.
- **Replicatie.** Gegevens kunnen gerepliceerd worden via een synchronisatieprotocol (éénweg replicatie), zodat de Opdrachtgever een eigen kopie kan bijhouden.
- **API-ontsluiting.** Gegevens kunnen via een API door de Opdrachtgever worden opgevraagd. De eisen voor die API staan in het document “API Richtlijnen”.
- **Documentatie van de datastructuur.** Up-to-date documentatie van de gebruikte datastructuur (datamodel, validatieschema) is beschikbaar voor de Opdrachtgever.
- **Exit verplichting — data-export (eis).** Bij beëindiging van de overeenkomst, ongeacht de reden, heeft de Opdrachtgever recht op volledige export van alle data in een open, machine leesbaar standaardformaat (minimaal JSON of CSV) binnen 30 dagen na beëindiging, kosteloos. De leverancier vernietigt de data aantoonbaar na succesvolle overdracht, conform de AVG.
- **Exit verplichting — overdrachtsperiode.** De leverancier verleent gedurende minimaal 90 dagen na contractbeëindiging medewerking aan een ordentelijke overgang naar een opvolgende leverancier of eigen beheer, inclusief technische ondersteuning bij de migratie.

✦ Aanbestedingseis
Eis: de Inschrijver beschrijft de exit-procedure: hoe wordt data geleverd, in welk formaat, binnen welke termijn, en op welke wijze de vernietiging nadien aantoonbaar wordt gemaakt.